



Bundesamt
für Sicherheit in der
Informationstechnik

Testdetailspezifikation für das Sicherheitsmodul nach BSI TR- 03109-2

BSI TR-03109-TS-2-Testdetailspezifikation

Version: 1.0

Datum : 06.03.2018



Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn

Tel.: +49 22899 9582-100

E-Mail: SmartMeter@bsi.bund.de

Internet: <https://www.bsi.bund.de>

© Bundesamt für Sicherheit in der Informationstechnik 2018

Inhaltsverzeichnis

1	Einleitung.....	72
1.1	Zielsetzung.....	73
1.2	Bezugsdokumente.....	73
1.3	Nomenklatur.....	73
1.4	Versionshistorie.....	74
2	Kommando-Tests.....	75
2.1	Testfall: ACTIVATE FILE (TC_ACTIVATE_FILE_GF_1).....	75
2.2	Testfall: ACTIVATE FILE (TC_ACTIVATE_FILE_FF_1).....	76
2.3	Testfall: ACTIVATE FILE (TC_ACTIVATE_FILE_FF_2).....	78
2.4	Testfall: ACTIVATE FILE (TC_ACTIVATE_FILE_FF_3).....	79
2.5	Testfall: ACTIVATE FILE (TC_ACTIVATE_FILE_FF_4_1).....	81
2.6	Testfall: ACTIVATE FILE (TC_ACTIVATE_FILE_FF_4_2).....	82
2.7	Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_GF_1_1).....	84
2.8	Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_GF_1_2).....	86
2.9	Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_GF_1_3).....	87
2.10	Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_GF_1_4).....	89
2.11	Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_1).....	91
2.12	Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_2_1).....	92
2.13	Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_2_2).....	94
2.14	Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_2_3).....	96
2.15	Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_2_4).....	97
2.16	Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_2_5).....	99
2.17	Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_2_6).....	101
2.18	Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_2_7).....	102
2.19	Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_2_8).....	104
2.20	Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_3_1).....	106
2.21	Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_3_2).....	107
2.22	Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_3_3).....	109
2.23	Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_3_4).....	111
2.24	Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_4_1).....	112
2.25	Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_4_2).....	114
2.26	Testfall: APPEND RECORD ohne SFI (TC_APPEND_RECORD_WITHOUT_SFI_GF_1).....	116
2.27	Testfall: APPEND RECORD ohne SFI (TC_APPEND_RECORD_WITHOUT_SFI_FF_1).....	117
2.28	Testfall: APPEND RECORD ohne SFI (TC_APPEND_RECORD_WITHOUT_SFI_FF_2).....	119
2.29	Testfall: APPEND RECORD ohne SFI (TC_APPEND_RECORD_WITHOUT_SFI_FF_3).....	121
2.30	Testfall: APPEND RECORD ohne SFI (TC_APPEND_RECORD_WITHOUT_SFI_FF_4).....	123
2.31	Testfall: APPEND RECORD ohne SFI (TC_APPEND_RECORD_WITHOUT_SFI_FF_5).....	125
2.32	Testfall: APPEND RECORD ohne SFI (TC_APPEND_RECORD_WITHOUT_SFI_FF_6).....	126
2.33	Testfall: APPEND RECORD ohne SFI (TC_APPEND_RECORD_WITHOUT_SFI_FF_7).....	128

2.34	Testfall: APPEND RECORD mit SFI (TC_APPEND_RECORD_WITH_SFI_GF_1).....	130
2.35	Testfall: APPEND RECORD mit SFI (TC_APPEND_RECORD_WITH_SFI_FF_1).....	132
2.36	Testfall: APPEND RECORD mit SFI (TC_APPEND_RECORD_WITH_SFI_FF_2).....	134
2.37	Testfall: APPEND RECORD mit SFI (TC_APPEND_RECORD_WITH_SFI_FF_3).....	136
2.38	Testfall: APPEND RECORD mit SFI (TC_APPEND_RECORD_WITH_SFI_FF_4).....	138
2.39	Testfall: APPEND RECORD mit SFI (TC_APPEND_RECORD_WITH_SFI_FF_5).....	140
2.40	Testfall: APPEND RECORD mit SFI (TC_APPEND_RECORD_WITH_SFI_FF_6).....	141
2.41	Testfall: APPEND RECORD mit SFI (TC_APPEND_RECORD_WITH_SFI_FF_7).....	143
2.42	Testfall: CHANGE REFERENCE DATA zum Wechseln der PIN (TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_GF_1_1).....	145
2.43	Testfall: CHANGE REFERENCE DATA zum Wechseln der PIN (TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_GF_1_2).....	147
2.44	Testfall: CHANGE REFERENCE DATA zum Wechseln der PIN (TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_GF_1_3).....	149
2.45	Testfall: CHANGE REFERENCE DATA zum Wechseln der PIN (TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_GF_2).....	151
2.46	Testfall: CHANGE REFERENCE DATA zum Wechseln der PIN (TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_1).....	153
2.47	Testfall: CHANGE REFERENCE DATA zum Wechseln der PIN (TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_2).....	155
2.48	Testfall: CHANGE REFERENCE DATA zum Wechseln der PIN (TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_3_1).....	157
2.49	Testfall: CHANGE REFERENCE DATA zum Wechseln der PIN (TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_3_2).....	159
2.50	Testfall: CHANGE REFERENCE DATA zum Wechseln der PIN (TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_4).....	161
2.51	Testfall: CHANGE REFERENCE DATA zum Wechseln der PIN (TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_5).....	162
2.52	Testfall: CHANGE REFERENCE DATA zum Wechseln der PIN (TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_6).....	164
2.53	Testfall: CHANGE REFERENCE DATA zum Setzen der PIN (TC_CHANGE_REFERENCE_DATA_SET_PIN_GF_1).....	166
2.54	Testfall: CHANGE REFERENCE DATA zum Setzen der PIN (TC_CHANGE_REFERENCE_DATA_SET_PIN_FF_1).....	168
2.55	Testfall: CHANGE REFERENCE DATA zum Setzen der PIN (TC_CHANGE_REFERENCE_DATA_SET_PIN_FF_2).....	169
2.56	Testfall: CHANGE REFERENCE DATA zum Setzen der PIN (TC_CHANGE_REFERENCE_DATA_SET_PIN_FF_3).....	171
2.57	Testfall: CREATE FILE (TC_CREATE_FILE_GF_1).....	172
2.58	Testfall: CREATE FILE (TC_CREATE_FILE_FF_1).....	174
2.59	Testfall: CREATE FILE (TC_CREATE_FILE_FF_2).....	176
2.60	Testfall: CREATE FILE (TC_CREATE_FILE_FF_3).....	178
2.61	Testfall: CREATE FILE (TC_CREATE_FILE_FF_4).....	179
2.62	Testfall: CREATE FILE (TC_CREATE_FILE_FF_5).....	181
2.63	Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_1).....	183

2.64	Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_2).....	185
2.65	Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_3).....	186
2.66	Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_4).....	188
2.67	Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_5).....	190
2.68	Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_6).....	192
2.69	Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_7).....	194
2.70	Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_8).....	195
2.71	Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_9).....	197
2.72	Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_10).....	199
2.73	Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_11).....	201
2.74	Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_12).....	203
2.75	Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_13).....	204
2.76	Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_14).....	206
2.77	Testfall: CREATE KEY (TC_CREATE_KEY_FF_1).....	208
2.78	Testfall: CREATE KEY (TC_CREATE_KEY_FF_2_1).....	210
2.79	Testfall: CREATE KEY (TC_CREATE_KEY_FF_2_2).....	211
2.80	Testfall: CREATE KEY (TC_CREATE_KEY_FF_3).....	213
2.81	Testfall: CREATE KEY (TC_CREATE_KEY_FF_4_1).....	215
2.82	Testfall: CREATE KEY (TC_CREATE_KEY_FF_4_2).....	217
2.83	Testfall: CREATE KEY (TC_CREATE_KEY_FF_4_3).....	219
2.84	Testfall: CREATE KEY (TC_CREATE_KEY_FF_4_4).....	220
2.85	Testfall: CREATE KEY (TC_CREATE_KEY_FF_4_5).....	222
2.86	Testfall: CREATE KEY (TC_CREATE_KEY_FF_4_6).....	224
2.87	Testfall: CREATE KEY (TC_CREATE_KEY_FF_4_7).....	226
2.88	Testfall: CREATE KEY (TC_CREATE_KEY_FF_4_8).....	228
2.89	Testfall: CREATE KEY (TC_CREATE_KEY_FF_5).....	229
2.90	Testfall: DEACTIVATE FILE (TC_DEACTIVATE_FILE_GF_1).....	231
2.91	Testfall: DEACTIVATE FILE (TC_DEACTIVATE_FILE_FF_1).....	233
2.92	Testfall: DEACTIVATE FILE (TC_DEACTIVATE_FILE_FF_2).....	234
2.93	Testfall: DEACTIVATE FILE (TC_DEACTIVATE_FILE_FF_3).....	236
2.94	Testfall: DEACTIVATE FILE (TC_DEACTIVATE_FILE_FF_4).....	237
2.95	Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_GF_1_1).....	239
2.96	Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_GF_1_2).....	241
2.97	Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_GF_1_3).....	242
2.98	Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_GF_1_4).....	244
2.99	Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_1).....	246
2.100	Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_2_1).....	248
2.101	Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_2_2).....	249
2.102	Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_2_3).....	251
2.103	Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_2_4).....	253
2.104	Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_3_1).....	254
2.105	Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_3_2).....	256

2.106	Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_4_1).....	258
2.107	Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_4_2).....	260
2.108	Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_4_3).....	261
2.109	Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_4_4).....	263
2.110	Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_4_5).....	265
2.111	Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_4_6).....	267
2.112	Testfall: DELETE FILE (TC_DELETE_FILE_GF_1).....	268
2.113	Testfall: DELETE FILE (TC_DELETE_FILE_FF_1).....	270
2.114	Testfall: DELETE FILE (TC_DELETE_FILE_FF_2).....	271
2.115	Testfall: DELETE FILE (TC_DELETE_FILE_FF_3).....	273
2.116	Testfall: DELETE KEY (TC_DELETE_KEY_GF_1_1).....	274
2.117	Testfall: DELETE KEY (TC_DELETE_KEY_GF_1_2).....	276
2.118	Testfall: DELETE KEY (TC_DELETE_KEY_GF_1_3).....	277
2.119	Testfall: DELETE KEY (TC_DELETE_KEY_GF_1_4).....	279
2.120	Testfall: DELETE KEY (TC_DELETE_KEY_FF_1).....	281
2.121	Testfall: DELETE KEY (TC_DELETE_KEY_FF_2_1).....	282
2.122	Testfall: DELETE KEY (TC_DELETE_KEY_FF_2_2).....	284
2.123	Testfall: DELETE KEY (TC_DELETE_KEY_FF_2_3).....	286
2.124	Testfall: DELETE KEY (TC_DELETE_KEY_FF_2_4).....	287
2.125	Testfall: DELETE KEY (TC_DELETE_KEY_FF_3_1).....	289
2.126	Testfall: DELETE KEY (TC_DELETE_KEY_FF_3_2).....	291
2.127	Testfall: DELETE KEY (TC_DELETE_KEY_FF_4_1).....	292
2.128	Testfall: DELETE KEY (TC_DELETE_KEY_FF_4_2).....	294
2.129	Testfall: DELETE KEY (TC_DELETE_KEY_FF_4_3).....	296
2.130	Testfall: DELETE KEY (TC_DELETE_KEY_FF_4_4).....	297
2.131	Testfall: DELETE KEY (TC_DELETE_KEY_FF_4_5).....	299
2.132	Testfall: DELETE KEY (TC_DELETE_KEY_FF_4_6).....	301
2.133	Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_GF_1_1).....	303
2.134	Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_GF_1_2).....	305
2.135	Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_GF_1_3).....	307
2.136	Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_GF_2_1).....	309
2.137	Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_GF_2_2).....	311
2.138	Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_GF_2_3).....	313
2.139	Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_1).....	315
2.140	Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_2).....	317
2.141	Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_3_1).....	319
2.142	Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_3_2).....	321
2.143	Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_4_1).....	323
2.144	Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_4_2).....	325
2.145	Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_4_3).....	327
2.146	Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_5).....	329
2.147	Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_6_1).....	331

2.148	Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_6_2).....	333
2.149	Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_6_3).....	335
2.150	Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_7_1).....	337
2.151	Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_7_2).....	339
2.152	Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_7_3).....	341
2.153	Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_8).....	343
2.154	Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_GF_1_1).....	345
2.155	Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_GF_1_2).....	347
2.156	Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_GF_2_1).....	349
2.157	Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_GF_2_2).....	351
2.158	Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_FF_1).....	353
2.159	Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_FF_2).....	355
2.160	Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_FF_3).....	358
2.161	Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_FF_4).....	360
2.162	Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_FF_5).....	362
2.163	Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_FF_6).....	364
2.164	Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_FF_7).....	367
2.165	Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_FF_8_1).....	369
2.166	Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_FF_8_2).....	371
2.167	Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_FF_8_3).....	373
2.168	Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_FF_8_4).....	376
2.169	Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_GF_1_1).....	378
2.170	Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_GF_1_2).....	380
2.171	Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_GF_1_3).....	381
2.172	Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_GF_1_4).....	383
2.173	Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_GF_2).....	385

2.174	Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_FF_1).....	387
2.175	Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_FF_2).....	389
2.176	Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_FF_3).....	391
2.177	Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_FF_4).....	393
2.178	Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_FF_5_1).....	394
2.179	Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_FF_5_2).....	396
2.180	Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_FF_5_3).....	398
2.181	Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_FF_5_4).....	400
2.182	Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_GF_1)	402
2.183	Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_1)	404
2.184	Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_2)	406
2.185	Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_3_1)	408
2.186	Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_3_2)	410
2.187	Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_4)	412
2.188	Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_1)	414
2.189	Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_2)	416
2.190	Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_3)	418
2.191	Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_4)	420

2.192	Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_5)	422
2.193	Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_6)	424
2.194	Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_7)	426
2.195	Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_8)	428
2.196	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_P UBLIC_KEY_GF_1_1)	430
2.197	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_P UBLIC_KEY_GF_1_2)	432
2.198	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_P UBLIC_KEY_GF_1_3)	434
2.199	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_P UBLIC_KEY_GF_1_4)	436
2.200	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_P UBLIC_KEY_GF_1_5)	438
2.201	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_P UBLIC_KEY_GF_1_6)	440
2.202	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_P UBLIC_KEY_GF_1_7)	442
2.203	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_P UBLIC_KEY_GF_1_8)	444
2.204	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_P UBLIC_KEY_FF_1)	446
2.205	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_P UBLIC_KEY_FF_2_1)	448
2.206	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_P UBLIC_KEY_FF_2_2)	450
2.207	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_P UBLIC_KEY_FF_2_3)	452

2.208	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_2_4).....	454
2.209	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_3_1).....	456
2.210	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_3_2).....	458
2.211	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_4).....	460
2.212	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_1).....	462
2.213	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_2).....	464
2.214	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_3).....	466
2.215	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_4).....	468
2.216	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_5).....	470
2.217	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_6).....	472
2.218	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_7).....	474
2.219	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_8).....	476
2.220	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_9).....	478
2.221	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_10).....	480
2.222	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_11).....	482
2.223	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_12).....	484

2.224	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_13).....	486
2.225	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_14).....	488
2.226	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_15).....	490
2.227	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_1).....	492
2.228	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_2).....	494
2.229	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_3).....	496
2.230	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_4).....	498
2.231	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_5).....	500
2.232	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_6).....	503
2.233	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_7).....	505
2.234	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_8).....	507
2.235	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_9).....	509
2.236	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_1).....	511
2.237	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_2_1).....	513
2.238	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_2_2).....	515
2.239	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_2_3).....	517

2.240	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_2_4).....	519
2.241	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_3_1).....	521
2.242	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_3_2).....	523
2.243	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_4).....	525
2.244	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_1).....	527
2.245	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_2).....	529
2.246	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_3).....	532
2.247	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_4).....	534
2.248	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_5).....	536
2.249	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_6).....	538
2.250	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_7).....	540
2.251	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_8).....	542
2.252	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_9).....	544
2.253	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_10).....	546
2.254	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_11).....	548
2.255	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_12).....	550

2.256	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_13).....	552
2.257	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_14).....	554
2.258	Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_15).....	556
2.259	Testfall: GET CHALLENGE (TC_GET_CHALLENGE_GF_1).....	558
2.260	Testfall: GET CHALLENGE (TC_GET_CHALLENGE_FF_1).....	559
2.261	Testfall: INTERNAL AUTHENTICATE (TC_INTERNAL_AUTHENTICATE_GF_1).....	561
2.262	Testfall: INTERNAL AUTHENTICATE (TC_INTERNAL_AUTHENTICATE_FF_1).....	563
2.263	Testfall: INTERNAL AUTHENTICATE (TC_INTERNAL_AUTHENTICATE_FF_2).....	565
2.264	Testfall: INTERNAL AUTHENTICATE (TC_INTERNAL_AUTHENTICATE_FF_3).....	567
2.265	Testfall: INTERNAL AUTHENTICATE (TC_INTERNAL_AUTHENTICATE_FF_4).....	569
2.266	Testfall: INTERNAL AUTHENTICATE (TC_INTERNAL_AUTHENTICATE_FF_5).....	571
2.267	Testfall: INTERNAL AUTHENTICATE (TC_INTERNAL_AUTHENTICATE_FF_6).....	573
2.268	Testfall: MANAGE CHANNEL (TC_MANAGE_CHANNEL_GF_1).....	575
2.269	Testfall: MANAGE CHANNEL (TC_MANAGE_CHANNEL_FF_1).....	576
2.270	Testfall: MSE RESTORE (TC_MSE_RESTORE_GF_1).....	577
2.271	Testfall: MSE RESTORE (TC_MSE_RESTORE_FF_1).....	579
2.272	Testfall: MSE SET mit CRT AT für externe Authentisierung (TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_GF_1).....	580
2.273	Testfall: MSE SET mit CRT AT für externe Authentisierung (TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_1).....	582
2.274	Testfall: MSE SET mit CRT AT für externe Authentisierung (TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_2).....	584
2.275	Testfall: MSE SET mit CRT AT für externe Authentisierung (TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_3_1).....	586
2.276	Testfall: MSE SET mit CRT AT für externe Authentisierung (TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_3_2).....	588
2.277	Testfall: MSE SET mit CRT AT für externe Authentisierung (TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_3_3).....	590
2.278	Testfall: MSE SET mit CRT AT für externe Authentisierung (TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_4).....	592
2.279	Testfall: MSE SET mit CRT AT für externe Authentisierung (TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_5).....	594
2.280	Testfall: MSE SET mit CRT AT für externe Authentisierung (TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_6_1).....	596
2.281	Testfall: MSE SET mit CRT AT für externe Authentisierung (TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_6_2).....	598
2.282	Testfall: MSE SET mit CRT AT für externe Authentisierung (TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_6_3).....	600

2.283	Testfall: MSE SET mit CRT AT für externe Authentisierung (TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_6_4).....	602
2.284	Testfall: MSE SET mit CRT AT für externe Authentisierung (TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_6_5).....	604
2.285	Testfall: MSE SET mit CRT AT für externe Authentisierung (TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_6_6).....	606
2.286	Testfall: MSE SET mit CRT AT für interne Authentisierung (TC_MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_GF_1).....	608
2.287	Testfall: MSE SET mit CRT AT für interne Authentisierung (TC_MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_1).....	610
2.288	Testfall: MSE SET mit CRT AT für interne Authentisierung (TC_MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_2).....	612
2.289	Testfall: MSE SET mit CRT AT für interne Authentisierung (TC_MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_3).....	614
2.290	Testfall: MSE SET mit CRT AT für interne Authentisierung (TC_MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_4).....	616
2.291	Testfall: MSE SET mit CRT AT für interne Authentisierung (TC_MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_5).....	618
2.292	Testfall: MSE SET mit CRT AT für interne Authentisierung (TC_MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_6_1).....	620
2.293	Testfall: MSE SET mit CRT AT für interne Authentisierung (TC_MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_6_2).....	622
2.294	Testfall: MSE SET mit CRT AT für interne Authentisierung (TC_MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_6_3).....	624
2.295	Testfall: MSE SET mit CRT AT für interne Authentisierung (TC_MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_6_4).....	626
2.296	Testfall: MSE SET mit CRT AT für interne Authentisierung (TC_MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_6_5).....	628
2.297	Testfall: MSE SET mit CRT AT für interne Authentisierung (TC_MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_6_6).....	630
2.298	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_GF_1_1).....	632
2.299	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_GF_1_2).....	634
2.300	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_GF_1_3).....	636
2.301	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_GF_1_4).....	638
2.302	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_1).....	640
2.303	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_2_1).....	642
2.304	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_2_2).....	645
2.305	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_2_3).....	647

2.306	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_2_4).....	649
2.307	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_3_1).....	651
2.308	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_3_2).....	653
2.309	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_3_3).....	655
2.310	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_3_4).....	657
2.311	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_4_1).....	660
2.312	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_4_2).....	662
2.313	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_4_3).....	664
2.314	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_4_4).....	667
2.315	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_5_1).....	669
2.316	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_5_2).....	671
2.317	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_5_3).....	674
2.318	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_5_4).....	676
2.319	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_1).....	678
2.320	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_2).....	680
2.321	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_3).....	682
2.322	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_4).....	685
2.323	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_5).....	687
2.324	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_6).....	689
2.325	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_7).....	691
2.326	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_8).....	693
2.327	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_9).....	695
2.328	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_10).....	698

2.329	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_11).....	700
2.330	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_12).....	702
2.331	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_13).....	705
2.332	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_14).....	707
2.333	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_15).....	709
2.334	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_16).....	712
2.335	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_17).....	714
2.336	Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_18).....	716
2.337	Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_GF_1).....	718
2.338	Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_FF_1).....	720
2.339	Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_FF_2).....	722
2.340	Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_FF_3).....	723
2.341	Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_FF_4_1).....	725
2.342	Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_FF_4_2).....	727
2.343	Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_FF_4_3).....	729
2.344	Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_FF_4_4).....	730
2.345	Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_FF_4_5).....	732
2.346	Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_FF_4_6).....	734
2.347	Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_FF_4_7).....	736
2.348	Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_FF_4_8).....	737
2.349	Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_FF_4_9).....	739
2.350	Testfall: MSE SET mit CRT DST für Signaturerzeugung (TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_GF_1).....	741
2.351	Testfall: MSE SET mit CRT DST für Signaturerzeugung (TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_1).....	743
2.352	Testfall: MSE SET mit CRT DST für Signaturerzeugung (TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_2).....	745
2.353	Testfall: MSE SET mit CRT DST für Signaturerzeugung (TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_3).....	747
2.354	Testfall: MSE SET mit CRT DST für Signaturerzeugung (TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_4).....	749
2.355	Testfall: MSE SET mit CRT DST für Signaturerzeugung (TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_5).....	751
2.356	Testfall: MSE SET mit CRT DST für Signaturerzeugung (TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_6_1).....	753
2.357	Testfall: MSE SET mit CRT DST für Signaturerzeugung (TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_6_2).....	755

2.358	Testfall: MSE SET mit CRT DST für Signaturerzeugung (TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_6_3).....	757
2.359	Testfall: MSE SET mit CRT DST für Signaturerzeugung (TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_6_4).....	759
2.360	Testfall: MSE SET mit CRT DST für Signaturerzeugung (TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_6_5).....	761
2.361	Testfall: MSE SET mit CRT DST für Signaturerzeugung (TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_6_6).....	763
2.362	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_GF_1).....	765
2.363	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_1_1).....	767
2.364	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_1_2).....	769
2.365	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_1_3).....	771
2.366	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_1_4).....	773
2.367	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_2_1).....	775
2.368	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_2_2).....	777
2.369	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_2_3).....	779
2.370	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_2_4).....	781
2.371	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_3_1).....	783
2.372	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_3_2).....	785
2.373	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_3_3).....	787
2.374	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_3_4).....	789
2.375	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_4_1).....	791
2.376	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_4_2).....	793
2.377	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_4_3).....	795
2.378	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_4_4).....	797
2.379	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_5_1).....	799
2.380	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_5_2).....	801

2.381	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_5_3).....	803
2.382	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_5_4).....	805
2.383	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_6_1).....	807
2.384	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_6_2).....	809
2.385	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_6_3).....	811
2.386	Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_6_4).....	813
2.387	Testfall: PSO COMPUTE DIGITAL SIGNATURE (TC_PSO_COMPUTE_DIGITAL_SIGNATURE_GF_1).....	815
2.388	Testfall: PSO COMPUTE DIGITAL SIGNATURE (TC_PSO_COMPUTE_DIGITAL_SIGNATURE_FF_1).....	817
2.389	Testfall: PSO COMPUTE DIGITAL SIGNATURE (TC_PSO_COMPUTE_DIGITAL_SIGNATURE_FF_2).....	819
2.390	Testfall: PSO COMPUTE DIGITAL SIGNATURE (TC_PSO_COMPUTE_DIGITAL_SIGNATURE_FF_3).....	821
2.391	Testfall: PSO COMPUTE DIGITAL SIGNATURE (TC_PSO_COMPUTE_DIGITAL_SIGNATURE_FF_4).....	823
2.392	Testfall: PSO COMPUTE DIGITAL SIGNATURE (TC_PSO_COMPUTE_DIGITAL_SIGNATURE_FF_5).....	825
2.393	Testfall: PSO COMPUTE DIGITAL SIGNATURE (TC_PSO_COMPUTE_DIGITAL_SIGNATURE_FF_6).....	827
2.394	Testfall: PSO COMPUTE DIGITAL SIGNATURE (TC_PSO_COMPUTE_DIGITAL_SIGNATURE_FF_7).....	829
2.395	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_GF_1_1).....	831
2.396	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_GF_1_2).....	833
2.397	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_GF_1_3).....	835
2.398	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_GF_1_4).....	837
2.399	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_GF_1_5).....	839
2.400	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_GF_2).....	841
2.401	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_1_1).....	843
2.402	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_1_2).....	846
2.403	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_1_3).....	848
2.404	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_1_4).....	850
2.405	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_1_5).....	852
2.406	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_2_1).....	854
2.407	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_2_2).....	857
2.408	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_2_3).....	859
2.409	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_2_4).....	861
2.410	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_2_5).....	863
2.411	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_3_1).....	865

2.412	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_3_2).....	868
2.413	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_3_3).....	870
2.414	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_3_4).....	872
2.415	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_3_5).....	874
2.416	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_4_1).....	876
2.417	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_4_2).....	879
2.418	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_4_3).....	881
2.419	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_4_4).....	883
2.420	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_4_5).....	885
2.421	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_5_1).....	887
2.422	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_5_2).....	890
2.423	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_5_3).....	892
2.424	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_5_4).....	894
2.425	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_5_5).....	896
2.426	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_6_1).....	899
2.427	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_6_2).....	901
2.428	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_6_3).....	903
2.429	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_6_4).....	905
2.430	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_6_5).....	907
2.431	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_7_1).....	910
2.432	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_7_2).....	912
2.433	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_7_3).....	914
2.434	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_7_4).....	916
2.435	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_7_5).....	918
2.436	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_1).....	921
2.437	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_2).....	923
2.438	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_3).....	925
2.439	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_4).....	927
2.440	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_5).....	929
2.441	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_6).....	932
2.442	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_7).....	934
2.443	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_8).....	936
2.444	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_9).....	938
2.445	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_10).....	940
2.446	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_11).....	943
2.447	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_12).....	945
2.448	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_13).....	947
2.449	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_14).....	949
2.450	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_15).....	951
2.451	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_16).....	954
2.452	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_17).....	956
2.453	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_18).....	958

2.454	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_19).....	960
2.455	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_20).....	962
2.456	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_21).....	965
2.457	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_22).....	967
2.458	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_23).....	969
2.459	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_24).....	971
2.460	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_9_1).....	973
2.461	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_9_2).....	976
2.462	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_9_3).....	978
2.463	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_9_4).....	980
2.464	Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_9_5).....	982
2.465	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_GF_1).....	984
2.466	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_GF_2_1).....	986
2.467	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_GF_2_2).....	988
2.468	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_GF_2_3).....	990
2.469	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_GF_2_4).....	992
2.470	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_GF_2_5).....	995
2.471	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_1_1).....	997
2.472	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_1_2).....	999
2.473	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_1_3).....	1001
2.474	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_1_4).....	1003
2.475	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_1_5).....	1005
2.476	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_2_1).....	1007

2.477	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_2_2).....	1009
2.478	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_2_3).....	1011
2.479	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_2_4).....	1013
2.480	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_2_5).....	1015
2.481	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_3_1).....	1017
2.482	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_3_2).....	1019
2.483	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_3_3).....	1021
2.484	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_3_4).....	1023
2.485	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_3_5).....	1025
2.486	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_4_1).....	1027
2.487	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_4_2).....	1029
2.488	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_4_3).....	1031
2.489	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_4_4).....	1033
2.490	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_4_5).....	1035
2.491	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_5_1).....	1037
2.492	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_5_2).....	1039

2.493	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_5_3).....	1041
2.494	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_5_4).....	1043
2.495	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_5_5).....	1045
2.496	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_6_1).....	1047
2.497	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_6_2).....	1049
2.498	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_6_3).....	1051
2.499	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_6_4).....	1053
2.500	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_6_5).....	1055
2.501	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_1).....	1057
2.502	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_2).....	1059
2.503	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_3).....	1061
2.504	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_4).....	1063
2.505	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_5).....	1065
2.506	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_6).....	1067
2.507	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_7).....	1069
2.508	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_8).....	1071

2.509	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_8_1).....	1073
2.510	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_8_2).....	1075
2.511	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_8_3).....	1077
2.512	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_8_4).....	1079
2.513	Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_8_5).....	1081
2.514	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_GF_1).....	1083
2.515	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_GF_2_1).....	1085
2.516	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_GF_2_2).....	1086
2.517	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_GF_2_3).....	1088
2.518	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_GF_2_4).....	1090
2.519	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_GF_2_5).....	1092
2.520	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_1_1).....	1094
2.521	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_1_2).....	1096
2.522	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_1_3).....	1098
2.523	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_1_4).....	1100
2.524	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_1_5).....	1102

2.525	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_2_1)	1104
2.526	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_2_2)	1106
2.527	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_2_3)	1108
2.528	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_2_4)	1110
2.529	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_2_5)	1112
2.530	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_1)	1114
2.531	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_2)	1116
2.532	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_3)	1118
2.533	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_4)	1120
2.534	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_5)	1122
2.535	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_6)	1124
2.536	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_7)	1126
2.537	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_8)	1128
2.538	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_4_1)	1130
2.539	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_4_2)	1132
2.540	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_4_3)	1134

2.541	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_4_4)	1136
2.542	Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_4_5)	1138
2.543	Testfall: READ BINARY ohne SFI (TC_READ_BINARY_WITHOUT_SFI_GF_1_1)	1139
2.544	Testfall: READ BINARY ohne SFI (TC_READ_BINARY_WITHOUT_SFI_GF_1_2)	1141
2.545	Testfall: READ BINARY ohne SFI (TC_READ_BINARY_WITHOUT_SFI_GF_1_3)	1143
2.546	Testfall: READ BINARY ohne SFI (TC_READ_BINARY_WITHOUT_SFI_FF_1)	1145
2.547	Testfall: READ BINARY ohne SFI (TC_READ_BINARY_WITHOUT_SFI_FF_2)	1146
2.548	Testfall: READ BINARY ohne SFI (TC_READ_BINARY_WITHOUT_SFI_GF_1)	1148
2.549	Testfall: READ BINARY ohne SFI (TC_READ_BINARY_WITHOUT_SFI_FF_1)	1150
2.550	Testfall: READ BINARY ohne SFI (TC_READ_BINARY_WITHOUT_SFI_FF_2)	1151
2.551	Testfall: READ BINARY mit SFI (TC_READ_BINARY_WITH_SFI_GF_1_1)	1153
2.552	Testfall: READ BINARY mit SFI (TC_READ_BINARY_WITH_SFI_GF_1_2)	1155
2.553	Testfall: READ BINARY mit SFI (TC_READ_BINARY_WITH_SFI_GF_1_3)	1157
2.554	Testfall: READ BINARY mit SFI (TC_READ_BINARY_WITH_SFI_FF_1)	1158
2.555	Testfall: READ BINARY mit SFI (TC_READ_BINARY_WITH_SFI_FF_2)	1160
2.556	Testfall: READ BINARY mit SFI (TC_READ_BINARY_WITH_SFI_FF_3)	1162
2.557	Testfall: READ BINARY mit SFI (TC_READ_BINARY_WITH_SFI_FF_4)	1164
2.558	Testfall: READ BINARY mit SFI (TC_READ_BINARY_WITH_SFI_FF_5)	1165
2.559	Testfall: READ RECORD ohne SFI (TC_READ_RECORD_WITHOUT_SFI_GF_1)	1167
2.560	Testfall: READ RECORD ohne SFI (TC_READ_RECORD_WITHOUT_SFI_FF_1)	1169
2.561	Testfall: READ RECORD ohne SFI (TC_READ_RECORD_WITHOUT_SFI_FF_2)	1171
2.562	Testfall: READ RECORD ohne SFI (TC_READ_RECORD_WITHOUT_SFI_FF_3)	1172
2.563	Testfall: READ RECORD ohne SFI (TC_READ_RECORD_WITHOUT_SFI_FF_4)	1174
2.564	Testfall: READ RECORD ohne SFI (TC_READ_RECORD_WITHOUT_SFI_FF_5)	1176
2.565	Testfall: READ RECORD mit SFI (TC_READ_RECORD_WITH_SFI_GF_1)	1178
2.566	Testfall: READ RECORD mit SFI (TC_READ_RECORD_WITH_SFI_FF_1)	1179
2.567	Testfall: READ RECORD mit SFI (TC_READ_RECORD_WITH_SFI_FF_2)	1181
2.568	Testfall: READ RECORD mit SFI (TC_READ_RECORD_WITH_SFI_FF_3)	1183
2.569	Testfall: READ RECORD mit SFI (TC_READ_RECORD_WITH_SFI_FF_4)	1185
2.570	Testfall: READ RECORD mit SFI (TC_READ_RECORD_WITH_SFI_FF_5)	1186
2.571	Testfall: SELECT eines DF mittels AID (TC_SELECT_DF_AID_GF_1_1)	1188
2.572	Testfall: SELECT eines DF mittels AID (TC_SELECT_DF_AID_GF_1_2)	1190
2.573	Testfall: SELECT eines DF mittels AID (TC_SELECT_DF_AID_GF_2_1)	1191
2.574	Testfall: SELECT eines DF mittels AID (TC_SELECT_DF_AID_GF_2_2)	1193
2.575	Testfall: SELECT eines DF mittels AID (TC_SELECT_DF_AID_GF_3)	1194
2.576	Testfall: SELECT eines DF mittels AID (TC_SELECT_DF_AID_FF_1)	1196
2.577	Testfall: SELECT eines DF mittels AID (TC_SELECT_DF_AID_FF_2)	1198
2.578	Testfall: SELECT eines DF mittels FID (TC_SELECT_DF_FID_GF_1)	1199
2.579	Testfall: SELECT eines DF mittels FID (TC_SELECT_DF_FID_GF_2)	1201

2.580	Testfall: SELECT eines DF mittels FID (TC_SELECT_DF_FID_GF_3).....	1202
2.581	Testfall: SELECT eines DF mittels FID (TC_SELECT_DF_FID_FF_1).....	1204
2.582	Testfall: SELECT eines DF mittels FID (TC_SELECT_DF_FID_FF_2).....	1205
2.583	Testfall: SELECT eines MF (TC_SELECT_DF_MF_GF_1).....	1207
2.584	Testfall: SELECT eines MF (TC_SELECT_DF_MF_FF_1).....	1208
2.585	Testfall: SELECT eines EF mittels FID (TC_SELECT_EF_GF_1).....	1209
2.586	Testfall: SELECT eines EF mittels FID (TC_SELECT_EF_GF_2).....	1211
2.587	Testfall: SELECT eines EF mittels FID (TC_SELECT_EF_GF_3).....	1213
2.588	Testfall: SELECT eines EF mittels FID (TC_SELECT_EF_FF_1).....	1214
2.589	Testfall: SELECT eines EF mittels FID (TC_SELECT_EF_FF_2).....	1216
2.590	Testfall: TERMINATE CARD USAGE (TC_TERMINATE_CARD_USAGE_GF_1).....	1217
2.591	Testfall: TERMINATE CARD USAGE (TC_TERMINATE_CARD_USAGE_FF_1).....	1219
2.592	Testfall: TERMINATE CARD USAGE (TC_TERMINATE_CARD_USAGE_FF_2).....	1220
2.593	Testfall: TERMINATE DF (TC_TERMINATE_DF_GF_1).....	1222
2.594	Testfall: TERMINATE DF (TC_TERMINATE_DF_FF_1).....	1223
2.595	Testfall: TERMINATE DF (TC_TERMINATE_DF_FF_2).....	1225
2.596	Testfall: TERMINATE DF (TC_TERMINATE_DF_FF_3).....	1226
2.597	Testfall: TERMINATE EF (TC_TERMINATE_EF_GF_1).....	1228
2.598	Testfall: TERMINATE EF (TC_TERMINATE_EF_FF_1).....	1229
2.599	Testfall: TERMINATE EF (TC_TERMINATE_EF_FF_2).....	1231
2.600	Testfall: TERMINATE EF (TC_TERMINATE_EF_FF_3).....	1232
2.601	Testfall: UPDATE BINARY ohne SFI (TC_UPDATE_BINARY_WITHOUT_SFI_GF_1).....	1234
2.602	Testfall: UPDATE BINARY ohne SFI (TC_UPDATE_BINARY_WITHOUT_SFI_FF_1).....	1235
2.603	Testfall: UPDATE BINARY ohne SFI (TC_UPDATE_BINARY_WITHOUT_SFI_FF_2).....	1237
2.604	Testfall: UPDATE BINARY ohne SFI (TC_UPDATE_BINARY_WITHOUT_SFI_FF_3).....	1239
2.605	Testfall: UPDATE BINARY ohne SFI (TC_UPDATE_BINARY_WITHOUT_SFI_FF_4).....	1241
2.606	Testfall: UPDATE BINARY ohne SFI (TC_UPDATE_BINARY_WITHOUT_SFI_FF_5).....	1243
2.607	Testfall: UPDATE BINARY ohne SFI (TC_UPDATE_BINARY_WITHOUT_SFI_FF_6).....	1245
2.608	Testfall: UPDATE BINARY mit SFI (TC_UPDATE_BINARY_WITH_SFI_GF_1).....	1247
2.609	Testfall: UPDATE BINARY mit SFI (TC_UPDATE_BINARY_WITH_SFI_FF_1).....	1248
2.610	Testfall: UPDATE BINARY mit SFI (TC_UPDATE_BINARY_WITH_SFI_FF_2).....	1250
2.611	Testfall: UPDATE BINARY mit SFI (TC_UPDATE_BINARY_WITH_SFI_FF_3).....	1252
2.612	Testfall: UPDATE BINARY mit SFI (TC_UPDATE_BINARY_WITH_SFI_FF_4).....	1254
2.613	Testfall: UPDATE BINARY mit SFI (TC_UPDATE_BINARY_WITH_SFI_FF_5).....	1256
2.614	Testfall: UPDATE BINARY mit SFI (TC_UPDATE_BINARY_WITH_SFI_FF_6).....	1258
2.615	Testfall: UPDATE RECORD ohne SFI (TC_UPDATE_RECORD_WITHOUT_SFI_GF_1)....	1260
2.616	Testfall: UPDATE RECORD ohne SFI (TC_UPDATE_RECORD_WITHOUT_SFI_FF_1).....	1262
2.617	Testfall: UPDATE RECORD ohne SFI (TC_UPDATE_RECORD_WITHOUT_SFI_FF_2).....	1264
2.618	Testfall: UPDATE RECORD ohne SFI (TC_UPDATE_RECORD_WITHOUT_SFI_FF_3).....	1266
2.619	Testfall: UPDATE RECORD ohne SFI (TC_UPDATE_RECORD_WITHOUT_SFI_FF_4).....	1268
2.620	Testfall: UPDATE RECORD ohne SFI (TC_UPDATE_RECORD_WITHOUT_SFI_FF_5).....	1270
2.621	Testfall: UPDATE RECORD ohne SFI (TC_UPDATE_RECORD_WITHOUT_SFI_FF_6).....	1272

2.622	Testfall: UPDATE RECORD ohne SFI (TC_UPDATE_RECORD_WITHOUT_SFI_FF_7).....	1274
2.623	Testfall: UPDATE RECORD mit SFI (TC_UPDATE_RECORD_WITH_SFI_GF_1).....	1276
2.624	Testfall: UPDATE RECORD mit SFI (TC_UPDATE_RECORD_WITH_SFI_FF_1).....	1278
2.625	Testfall: UPDATE RECORD mit SFI (TC_UPDATE_RECORD_WITH_SFI_FF_2).....	1280
2.626	Testfall: UPDATE RECORD mit SFI (TC_UPDATE_RECORD_WITH_SFI_FF_3).....	1282
2.627	Testfall: UPDATE RECORD mit SFI (TC_UPDATE_RECORD_WITH_SFI_FF_4).....	1284
2.628	Testfall: UPDATE RECORD mit SFI (TC_UPDATE_RECORD_WITH_SFI_FF_5).....	1286
2.629	Testfall: UPDATE RECORD mit SFI (TC_UPDATE_RECORD_WITH_SFI_FF_6).....	1288
2.630	Testfall: UPDATE RECORD mit SFI (TC_UPDATE_RECORD_WITH_SFI_FF_7).....	1290
3	Funktions-Tests.....	1292
3.1	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_1).....	1292
3.2	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_2_1).....	1293
3.3	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_2_2).....	1294
3.4	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_2_3).....	1295
3.5	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_2_4).....	1296
3.6	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_3a_1).....	1297
3.7	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_3a_2).....	1298
3.8	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_3a_3).....	1299
3.9	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_3a_4).....	1300
3.10	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_3a_5).....	1301
3.11	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_3a_6).....	1302
3.12	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_3b_7).....	1303
3.13	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_3b_8).....	1304
3.14	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_3c_9).....	1305
3.15	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_3c_10).....	1306
3.16	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_3c_11).....	1307
3.17	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_3c_12).....	1308
3.18	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_4).....	1309
3.19	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_5).....	1310
3.20	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_6_1).....	1311
3.21	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_6_2).....	1312
3.22	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_6_3).....	1313
3.23	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_6_4).....	1314
3.24	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_6_5).....	1315
3.25	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_7a_1).....	1316
3.26	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_7a_2).....	1317
3.27	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_7b_3).....	1318
3.28	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_7b_4).....	1319
3.29	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_7b_5).....	1320
3.30	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_7b_6).....	1321
3.31	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_7c_7).....	1322
3.32	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_7c_8).....	1323

3.33	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_7c_9).....	1324
3.34	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_7c_10).....	1325
3.35	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_11_1).....	1326
3.36	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_12_2).....	1328
3.37	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_13_3).....	1329
3.38	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_9a_1).....	1330
3.39	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_9a_2).....	1331
3.40	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_9a_3).....	1332
3.41	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_9a_4).....	1333
3.42	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_9a_5).....	1335
3.43	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_9a_6).....	1336
3.44	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_9b_7).....	1337
3.45	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_9b_8).....	1338
3.46	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_9c_9).....	1339
3.47	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_9c_10).....	1340
3.48	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_9c_11).....	1341
3.49	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_9c_12).....	1343
3.50	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_10a_13).....	1344
3.51	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_10a_14).....	1345
3.52	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_10b_15).....	1346
3.53	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_10b_16).....	1347
3.54	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_10b_17).....	1348
3.55	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_10b_18).....	1350
3.56	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_10c_19).....	1351
3.57	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_10c_20).....	1352
3.58	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_10c_21).....	1353
3.59	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_10c_22).....	1354
3.60	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_1).....	1355
3.61	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_2).....	1356
3.62	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_3).....	1357
3.63	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_4).....	1359
3.64	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_5).....	1360
3.65	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_6).....	1361
3.66	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_7).....	1362
3.67	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_8).....	1363
3.68	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_9).....	1364
3.69	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_10).....	1365
3.70	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_11).....	1366
3.71	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_12).....	1367
3.72	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_13).....	1368
3.73	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_14).....	1369
3.74	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_15).....	1370

3.75	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_16).....	1371
3.76	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_17).....	1372
3.77	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_18).....	1373
3.78	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_19).....	1374
3.79	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_20).....	1375
3.80	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_21).....	1376
3.81	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_22).....	1377
3.82	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_23).....	1378
3.83	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_24).....	1379
3.84	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_25).....	1380
3.85	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_26).....	1381
3.86	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_27).....	1382
3.87	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_28).....	1384
3.88	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_29).....	1385
3.89	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_30).....	1386
3.90	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_31).....	1387
3.91	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_32).....	1388
3.92	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_33).....	1389
3.93	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_34).....	1390
3.94	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_35).....	1391
3.95	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_36).....	1392
3.96	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_37).....	1393
3.97	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_38).....	1394
3.98	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_39).....	1395
3.99	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_40).....	1396
3.100	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_41).....	1397
3.101	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_42).....	1398
3.102	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_43).....	1400
3.103	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_44).....	1401
3.104	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_45).....	1402
3.105	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_46).....	1403
3.106	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_47).....	1404
3.107	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_48).....	1405
3.108	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_49).....	1406
3.109	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_50).....	1407
3.110	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_51).....	1408
3.111	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_52).....	1409
3.112	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_53).....	1410
3.113	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_54).....	1411
3.114	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_55).....	1413
3.115	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_56).....	1414
3.116	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_57).....	1415

3.117	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_58).....	1416
3.118	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_59).....	1417
3.119	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_60).....	1418
3.120	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_61).....	1419
3.121	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_62).....	1421
3.122	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_63).....	1422
3.123	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_64).....	1423
3.124	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_65).....	1424
3.125	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_66).....	1425
3.126	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_67).....	1426
3.127	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_68).....	1428
3.128	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_69).....	1429
3.129	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_70).....	1430
3.130	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_71).....	1431
3.131	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_72).....	1432
3.132	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_73).....	1433
3.133	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_74).....	1434
3.134	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_75).....	1436
3.135	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_76).....	1437
3.136	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_77).....	1438
3.137	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_78).....	1439
3.138	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_79).....	1440
3.139	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_80).....	1441
3.140	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_81).....	1442
3.141	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_82).....	1443
3.142	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_83).....	1445
3.143	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_84).....	1446
3.144	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_85).....	1447
3.145	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_86).....	1448
3.146	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_87).....	1449
3.147	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_88).....	1450
3.148	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_89).....	1451
3.149	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_90).....	1452
3.150	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_91).....	1454
3.151	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_92).....	1455
3.152	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_93).....	1456
3.153	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_94).....	1457
3.154	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_95).....	1458
3.155	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_96).....	1460
3.156	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_97).....	1461
3.157	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_98).....	1462
3.158	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_99).....	1463

3.159	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_100).....	1464
3.160	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_101).....	1466
3.161	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_102).....	1467
3.162	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_103).....	1468
3.163	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_104).....	1469
3.164	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_105).....	1470
3.165	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_106).....	1471
3.166	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_107).....	1472
3.167	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_108).....	1473
3.168	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_109).....	1475
3.169	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_110).....	1476
3.170	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_111).....	1477
3.171	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_112).....	1478
3.172	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_113).....	1479
3.173	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_114).....	1480
3.174	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_115).....	1481
3.175	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_116).....	1482
3.176	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_117).....	1484
3.177	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_118).....	1485
3.178	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_119).....	1486
3.179	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_120).....	1487
3.180	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_121).....	1488
3.181	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_122).....	1489
3.182	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_123).....	1490
3.183	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_124).....	1492
3.184	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_125).....	1493
3.185	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_126).....	1494
3.186	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_127).....	1495
3.187	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_128).....	1496
3.188	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_129).....	1497
3.189	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_130).....	1499
3.190	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_131).....	1500
3.191	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_132).....	1501
3.192	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_133).....	1502
3.193	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_134).....	1503
3.194	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_135).....	1504
3.195	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_136).....	1505
3.196	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_137).....	1507
3.197	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_138).....	1508
3.198	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_139).....	1509
3.199	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_140).....	1510
3.200	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_141).....	1511

3.201	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_142).....	1512
3.202	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_143).....	1513
3.203	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_144).....	1514
3.204	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_145).....	1516
3.205	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_146).....	1517
3.206	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_147).....	1518
3.207	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_148).....	1519
3.208	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_149).....	1520
3.209	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_150).....	1521
3.210	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_151).....	1522
3.211	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_152).....	1523
3.212	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_153).....	1525
3.213	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_154).....	1526
3.214	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_155).....	1527
3.215	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_156).....	1528
3.216	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_157).....	1529
3.217	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_158).....	1531
3.218	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_159).....	1532
3.219	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_160).....	1533
3.220	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_161).....	1534
3.221	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_162).....	1535
3.222	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_163).....	1537
3.223	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_164).....	1538
3.224	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_165).....	1539
3.225	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_166).....	1540
3.226	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_167).....	1541
3.227	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_168).....	1542
3.228	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_169).....	1543
3.229	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_170).....	1544
3.230	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_171).....	1546
3.231	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_172).....	1547
3.232	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_173).....	1548
3.233	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_174).....	1549
3.234	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_175).....	1550
3.235	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_176).....	1551
3.236	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_177).....	1552
3.237	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_178).....	1553
3.238	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_179).....	1555
3.239	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_180).....	1556
3.240	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_181).....	1557
3.241	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_182).....	1558
3.242	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_183).....	1559

3.243	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_184).....	1560
3.244	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_185).....	1561
3.245	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_186).....	1563
3.246	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_187).....	1564
3.247	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_188).....	1565
3.248	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_189).....	1566
3.249	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_190).....	1567
3.250	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_191).....	1568
3.251	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_192).....	1570
3.252	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_193).....	1571
3.253	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_194).....	1572
3.254	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_195).....	1573
3.255	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_196).....	1574
3.256	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_197).....	1575
3.257	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_198).....	1576
3.258	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_199).....	1578
3.259	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_200).....	1579
3.260	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_201).....	1580
3.261	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_202).....	1581
3.262	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_203).....	1582
3.263	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_204).....	1583
3.264	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_205).....	1584
3.265	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_206).....	1585
3.266	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_207).....	1587
3.267	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_208).....	1588
3.268	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_209).....	1589
3.269	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_210).....	1590
3.270	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_211).....	1591
3.271	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_212).....	1592
3.272	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_213).....	1593
3.273	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_214).....	1594
3.274	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_215).....	1596
3.275	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_216).....	1597
3.276	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_217).....	1598
3.277	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_218).....	1599
3.278	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_219).....	1600
3.279	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_220).....	1602
3.280	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_221).....	1603
3.281	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_222).....	1604
3.282	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_223).....	1605
3.283	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_224).....	1606
3.284	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_225).....	1608

3.285	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_226).....	1609
3.286	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_227).....	1610
3.287	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_228).....	1611
3.288	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_229).....	1612
3.289	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_230).....	1613
3.290	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_231).....	1614
3.291	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_232).....	1615
3.292	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_233).....	1617
3.293	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_234).....	1618
3.294	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_235).....	1619
3.295	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_236).....	1620
3.296	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_237).....	1621
3.297	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_238).....	1622
3.298	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_239).....	1623
3.299	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_240).....	1624
3.300	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_241).....	1626
3.301	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_242).....	1627
3.302	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_243).....	1628
3.303	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_244).....	1629
3.304	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_245).....	1630
3.305	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_246).....	1631
3.306	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_247).....	1632
3.307	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_248).....	1634
3.308	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_249).....	1635
3.309	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_250).....	1636
3.310	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_251).....	1637
3.311	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_252).....	1638
3.312	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_253).....	1639
3.313	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_254).....	1641
3.314	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_255).....	1642
3.315	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_256).....	1643
3.316	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_257).....	1644
3.317	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_258).....	1645
3.318	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_259).....	1646
3.319	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_260).....	1647
3.320	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_261).....	1649
3.321	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_262).....	1650
3.322	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_263).....	1651
3.323	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_264).....	1652
3.324	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_265).....	1653
3.325	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_266).....	1654
3.326	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_267).....	1655

3.327	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_268).....	1656
3.328	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_269).....	1658
3.329	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_270).....	1659
3.330	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_271).....	1660
3.331	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_272).....	1661
3.332	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_273).....	1662
3.333	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_274).....	1663
3.334	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_275).....	1664
3.335	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_276).....	1665
3.336	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_277).....	1667
3.337	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_278).....	1668
3.338	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_279).....	1669
3.339	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_280).....	1670
3.340	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_281).....	1671
3.341	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_282).....	1673
3.342	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_283).....	1674
3.343	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_284).....	1675
3.344	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_285).....	1676
3.345	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_286).....	1677
3.346	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_287).....	1679
3.347	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_288).....	1680
3.348	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_289).....	1681
3.349	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_290).....	1682
3.350	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_291).....	1683
3.351	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_292).....	1684
3.352	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_293).....	1685
3.353	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_294).....	1686
3.354	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_295).....	1688
3.355	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_296).....	1689
3.356	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_297).....	1690
3.357	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_298).....	1691
3.358	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_299).....	1692
3.359	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_300).....	1693
3.360	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_301).....	1694
3.361	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_302).....	1695
3.362	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_303).....	1697
3.363	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_304).....	1698
3.364	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_305).....	1699
3.365	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_306).....	1700
3.366	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_307).....	1701
3.367	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_308).....	1702
3.368	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_309).....	1703

3.369	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_310).....	1705
3.370	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_311).....	1706
3.371	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_312).....	1707
3.372	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_313).....	1708
3.373	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_314).....	1709
3.374	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_315).....	1710
3.375	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_316).....	1712
3.376	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_317).....	1713
3.377	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_318).....	1714
3.378	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_319).....	1715
3.379	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_320).....	1716
3.380	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_321).....	1717
3.381	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_322).....	1718
3.382	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_323).....	1720
3.383	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_324).....	1721
3.384	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_325).....	1722
3.385	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_326).....	1723
3.386	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_327).....	1724
3.387	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_328).....	1725
3.388	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_329).....	1726
3.389	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_330).....	1727
3.390	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_331).....	1729
3.391	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_332).....	1730
3.392	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_333).....	1731
3.393	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_334).....	1732
3.394	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_335).....	1733
3.395	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_336).....	1734
3.396	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_337).....	1735
3.397	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_338).....	1737
3.398	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_339).....	1738
3.399	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_340).....	1739
3.400	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_341).....	1740
3.401	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_342).....	1741
3.402	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_343).....	1743
3.403	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_344).....	1744
3.404	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_345).....	1745
3.405	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_346).....	1746
3.406	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_347).....	1747
3.407	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_348).....	1749
3.408	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_349).....	1750
3.409	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_350).....	1751
3.410	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_351).....	1752

3.411	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_352).....	1753
3.412	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_353).....	1754
3.413	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_354).....	1755
3.414	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_355).....	1756
3.415	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_356).....	1758
3.416	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_357).....	1759
3.417	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_358).....	1760
3.418	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_359).....	1761
3.419	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_360).....	1762
3.420	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_361).....	1763
3.421	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_362).....	1764
3.422	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_363).....	1765
3.423	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_364).....	1766
3.424	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_365).....	1767
3.425	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_366).....	1769
3.426	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_367).....	1770
3.427	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_368).....	1771
3.428	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_369).....	1772
3.429	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_370).....	1773
3.430	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_371).....	1775
3.431	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_372).....	1776
3.432	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_373).....	1777
3.433	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_374).....	1778
3.434	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_375).....	1779
3.435	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_376).....	1780
3.436	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_377).....	1781
3.437	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_378).....	1783
3.438	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_379).....	1784
3.439	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_380).....	1785
3.440	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_381).....	1786
3.441	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_382).....	1787
3.442	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_383).....	1788
3.443	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_384).....	1789
3.444	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_385).....	1790
3.445	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_386).....	1792
3.446	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_387).....	1793
3.447	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_388).....	1794
3.448	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_389).....	1795
3.449	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_390).....	1796
3.450	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_391).....	1797
3.451	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_392).....	1798
3.452	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_393).....	1800

3.453	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_394).....	1801
3.454	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_395).....	1802
3.455	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_396).....	1803
3.456	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_397).....	1804
3.457	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_398).....	1805
3.458	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_399).....	1807
3.459	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_400).....	1808
3.460	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_401).....	1809
3.461	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_402).....	1810
3.462	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_403).....	1811
3.463	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_404).....	1812
3.464	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_405).....	1814
3.465	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_406).....	1815
3.466	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_407).....	1816
3.467	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_408).....	1817
3.468	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_409).....	1818
3.469	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_410).....	1819
3.470	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_411).....	1820
3.471	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_412).....	1822
3.472	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_413).....	1823
3.473	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_414).....	1824
3.474	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_415).....	1825
3.475	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_416).....	1826
3.476	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_417).....	1827
3.477	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_418).....	1828
3.478	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_419).....	1829
3.479	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_420).....	1830
3.480	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_421).....	1831
3.481	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_422).....	1832
3.482	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_423).....	1833
3.483	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_424).....	1834
3.484	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_425).....	1835
3.485	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_426).....	1836
3.486	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_427).....	1837
3.487	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_428).....	1838
3.488	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_429).....	1839
3.489	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_430).....	1840
3.490	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_431).....	1841
3.491	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_432).....	1842
3.492	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_433).....	1844
3.493	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_434).....	1845
3.494	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_435).....	1846

3.495	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_436).....	1847
3.496	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_437).....	1848
3.497	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_438).....	1849
3.498	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_439).....	1850
3.499	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_440).....	1851
3.500	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_441).....	1852
3.501	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_442).....	1853
3.502	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_443).....	1854
3.503	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_444).....	1855
3.504	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_445).....	1856
3.505	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_446).....	1857
3.506	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_447).....	1858
3.507	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_448).....	1859
3.508	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_449).....	1860
3.509	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_450).....	1861
3.510	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_451).....	1862
3.511	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_452).....	1863
3.512	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_453).....	1864
3.513	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_454).....	1865
3.514	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_455).....	1866
3.515	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_456).....	1867
3.516	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_457).....	1868
3.517	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_458).....	1869
3.518	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_459).....	1870
3.519	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_460).....	1871
3.520	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_461).....	1872
3.521	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_462).....	1873
3.522	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_463).....	1875
3.523	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_464).....	1876
3.524	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_465).....	1877
3.525	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_466).....	1879
3.526	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_467).....	1880
3.527	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_468).....	1881
3.528	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_469).....	1882
3.529	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_470).....	1883
3.530	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_471).....	1885
3.531	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_472).....	1886
3.532	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_473).....	1887
3.533	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_474).....	1888
3.534	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_475).....	1889
3.535	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_476).....	1890
3.536	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_477).....	1891

3.537	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_478).....	1892
3.538	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_479).....	1893
3.539	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_480).....	1894
3.540	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_481).....	1895
3.541	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_482).....	1896
3.542	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_483).....	1897
3.543	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_484).....	1898
3.544	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_485).....	1899
3.545	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_486).....	1900
3.546	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_487).....	1901
3.547	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_488).....	1902
3.548	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_489).....	1903
3.549	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_490).....	1904
3.550	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_491).....	1905
3.551	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_492).....	1906
3.552	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_493).....	1908
3.553	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_494).....	1909
3.554	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_495).....	1910
3.555	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_496).....	1911
3.556	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_497).....	1912
3.557	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_498).....	1913
3.558	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_499).....	1914
3.559	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_500).....	1915
3.560	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_501).....	1916
3.561	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_502).....	1917
3.562	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_503).....	1918
3.563	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_504).....	1919
3.564	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_505).....	1920
3.565	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_506).....	1921
3.566	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_507).....	1922
3.567	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_508).....	1923
3.568	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_509).....	1924
3.569	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_510).....	1926
3.570	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_511).....	1927
3.571	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_512).....	1928
3.572	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_513).....	1929
3.573	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_514).....	1930
3.574	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_515).....	1931
3.575	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_516).....	1932
3.576	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_517).....	1933
3.577	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_518).....	1934
3.578	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_519).....	1935

3.579	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_520).....	1936
3.580	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_521).....	1937
3.581	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_522).....	1938
3.582	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_523).....	1939
3.583	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_524).....	1940
3.584	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_525).....	1941
3.585	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_526).....	1943
3.586	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_527).....	1944
3.587	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_528).....	1945
3.588	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_529).....	1946
3.589	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_530).....	1947
3.590	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_531).....	1948
3.591	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_532).....	1949
3.592	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_533).....	1950
3.593	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_534).....	1951
3.594	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_535).....	1953
3.595	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_536).....	1954
3.596	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_537).....	1955
3.597	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_538).....	1956
3.598	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_539).....	1957
3.599	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_540).....	1958
3.600	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_541).....	1959
3.601	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_542).....	1961
3.602	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_543).....	1962
3.603	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_544).....	1963
3.604	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_545).....	1964
3.605	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_546).....	1965
3.606	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_547).....	1966
3.607	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_548).....	1967
3.608	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_549).....	1969
3.609	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_550).....	1970
3.610	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_551).....	1971
3.611	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_552).....	1972
3.612	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_553).....	1973
3.613	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_554).....	1974
3.614	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_555).....	1975
3.615	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_556).....	1976
3.616	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_557).....	1978
3.617	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_558).....	1979
3.618	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_559).....	1980
3.619	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_560).....	1981
3.620	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_561).....	1982

3.621	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_562).....	1983
3.622	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_563).....	1985
3.623	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_564).....	1986
3.624	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_565).....	1987
3.625	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_566).....	1988
3.626	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_567).....	1989
3.627	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_568).....	1990
3.628	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_569).....	1991
3.629	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_570).....	1992
3.630	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_571).....	1994
3.631	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_572).....	1995
3.632	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_573).....	1996
3.633	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_574).....	1997
3.634	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_575).....	1998
3.635	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_576).....	1999
3.636	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_577).....	2000
3.637	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_578).....	2001
3.638	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_579).....	2003
3.639	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_580).....	2004
3.640	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_581).....	2005
3.641	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_582).....	2006
3.642	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_583).....	2007
3.643	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_584).....	2008
3.644	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_585).....	2009
3.645	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_586).....	2011
3.646	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_587).....	2012
3.647	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_588).....	2013
3.648	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_589).....	2014
3.649	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_590).....	2015
3.650	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_591).....	2016
3.651	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_592).....	2018
3.652	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_593).....	2019
3.653	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_594).....	2020
3.654	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_595).....	2021
3.655	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_596).....	2022
3.656	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_597).....	2023
3.657	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_598).....	2024
3.658	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_599).....	2026
3.659	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_600).....	2027
3.660	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_601).....	2028
3.661	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_602).....	2029
3.662	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_603).....	2030

3.663	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_604).....	2031
3.664	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_605).....	2032
3.665	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_606).....	2033
3.666	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_607).....	2035
3.667	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_608).....	2036
3.668	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_609).....	2037
3.669	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_610).....	2038
3.670	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_611).....	2039
3.671	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_612).....	2040
3.672	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_613).....	2041
3.673	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_614).....	2042
3.674	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_615).....	2043
3.675	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_616).....	2045
3.676	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_617).....	2046
3.677	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_618).....	2047
3.678	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_619).....	2048
3.679	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_620).....	2049
3.680	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_621).....	2051
3.681	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_622).....	2052
3.682	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_623).....	2053
3.683	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_624).....	2054
3.684	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_625).....	2055
3.685	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_626).....	2056
3.686	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_627).....	2058
3.687	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_628).....	2059
3.688	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_629).....	2060
3.689	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_630).....	2061
3.690	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_631).....	2062
3.691	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_632).....	2063
3.692	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_633).....	2064
3.693	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_634).....	2065
3.694	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_635).....	2066
3.695	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_636).....	2068
3.696	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_637).....	2069
3.697	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_638).....	2070
3.698	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_639).....	2071
3.699	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_640).....	2072
3.700	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_641).....	2073
3.701	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_642).....	2074
3.702	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_643).....	2075
3.703	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_644).....	2077
3.704	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_645).....	2078

3.705	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_646).....	2079
3.706	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_647).....	2080
3.707	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_648).....	2081
3.708	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_649).....	2082
3.709	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_650).....	2083
3.710	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_651).....	2084
3.711	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_652).....	2085
3.712	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_653).....	2087
3.713	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_654).....	2088
3.714	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_655).....	2089
3.715	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_656).....	2090
3.716	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_657).....	2091
3.717	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_658).....	2092
3.718	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_659).....	2093
3.719	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_660).....	2095
3.720	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_661).....	2096
3.721	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_662).....	2097
3.722	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_663).....	2098
3.723	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_664).....	2099
3.724	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_665).....	2100
3.725	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_666).....	2102
3.726	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_667).....	2103
3.727	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_668).....	2104
3.728	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_669).....	2105
3.729	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_670).....	2106
3.730	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_671).....	2107
3.731	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_672).....	2108
3.732	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_673).....	2109
3.733	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_674).....	2111
3.734	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_675).....	2112
3.735	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_676).....	2113
3.736	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_677).....	2114
3.737	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_678).....	2115
3.738	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_679).....	2116
3.739	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_680).....	2117
3.740	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_681).....	2118
3.741	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_682).....	2119
3.742	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_683).....	2121
3.743	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_684).....	2122
3.744	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_685).....	2123
3.745	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_686).....	2124
3.746	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_687).....	2125

3.747	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_688).....	2126
3.748	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_689).....	2127
3.749	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_690).....	2129
3.750	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_691).....	2130
3.751	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_692).....	2131
3.752	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_693).....	2132
3.753	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_694).....	2133
3.754	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_695).....	2134
3.755	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_696).....	2135
3.756	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_697).....	2137
3.757	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_698).....	2138
3.758	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_699).....	2139
3.759	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_700).....	2140
3.760	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_701).....	2141
3.761	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_702).....	2142
3.762	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_703).....	2143
3.763	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_704).....	2144
3.764	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_705).....	2146
3.765	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_706).....	2147
3.766	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_707).....	2148
3.767	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_708).....	2149
3.768	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_709).....	2150
3.769	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_710).....	2151
3.770	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_711).....	2152
3.771	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_712).....	2153
3.772	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_713).....	2155
3.773	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_714).....	2156
3.774	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_715).....	2157
3.775	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_716).....	2158
3.776	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_717).....	2159
3.777	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_718).....	2160
3.778	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_719).....	2161
3.779	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_720).....	2162
3.780	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_721).....	2163
3.781	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_722).....	2165
3.782	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_723).....	2166
3.783	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_724).....	2167
3.784	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_725).....	2168
3.785	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_726).....	2169
3.786	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_727).....	2170
3.787	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_728).....	2172
3.788	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_729).....	2173

3.789	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_730).....	2174
3.790	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_731).....	2175
3.791	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_732).....	2176
3.792	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_733).....	2177
3.793	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_734).....	2179
3.794	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_735).....	2180
3.795	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_736).....	2181
3.796	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_737).....	2182
3.797	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_738).....	2183
3.798	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_739).....	2184
3.799	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_740).....	2185
3.800	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_741).....	2186
3.801	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_742).....	2188
3.802	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_743).....	2189
3.803	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_744).....	2190
3.804	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_745).....	2191
3.805	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_746).....	2192
3.806	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_747).....	2193
3.807	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_748).....	2194
3.808	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_749).....	2195
3.809	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_750).....	2197
3.810	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_751).....	2198
3.811	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_752).....	2199
3.812	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_753).....	2200
3.813	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_754).....	2201
3.814	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_755).....	2202
3.815	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_756).....	2203
3.816	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_757).....	2204
3.817	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_758).....	2205
3.818	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_759).....	2206
3.819	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_760).....	2208
3.820	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_761).....	2209
3.821	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_762).....	2210
3.822	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_763).....	2211
3.823	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_764).....	2212
3.824	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_765).....	2214
3.825	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_766).....	2215
3.826	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_767).....	2216
3.827	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_768).....	2217
3.828	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_769).....	2218
3.829	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_770).....	2219
3.830	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_771).....	2221

3.831	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_772).....	2222
3.832	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_773).....	2223
3.833	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_774).....	2224
3.834	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_775).....	2225
3.835	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_776).....	2226
3.836	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_777).....	2227
3.837	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_778).....	2228
3.838	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_779).....	2229
3.839	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_780).....	2230
3.840	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_781).....	2232
3.841	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_782).....	2233
3.842	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_783).....	2234
3.843	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_784).....	2235
3.844	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_785).....	2236
3.845	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_786).....	2237
3.846	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_787).....	2238
3.847	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_788).....	2239
3.848	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_789).....	2240
3.849	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_790).....	2242
3.850	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_791).....	2243
3.851	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_792).....	2244
3.852	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_793).....	2245
3.853	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_794).....	2246
3.854	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_795).....	2247
3.855	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_796).....	2248
3.856	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_797).....	2250
3.857	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_798).....	2251
3.858	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_799).....	2252
3.859	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_800).....	2253
3.860	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_801).....	2254
3.861	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_802).....	2255
3.862	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_803).....	2256
3.863	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_804).....	2258
3.864	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_805).....	2259
3.865	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_806).....	2260
3.866	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_807).....	2261
3.867	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_808).....	2262
3.868	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_809).....	2263
3.869	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_810).....	2264
3.870	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_811).....	2265
3.871	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_812).....	2267
3.872	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_813).....	2268

3.873	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_814).....	2269
3.874	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_815).....	2270
3.875	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_1).....	2271
3.876	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_2).....	2272
3.877	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_3).....	2273
3.878	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_4).....	2274
3.879	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_5).....	2275
3.880	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_6).....	2277
3.881	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_7).....	2278
3.882	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_8).....	2279
3.883	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_9).....	2280
3.884	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_10).....	2281
3.885	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_11).....	2282
3.886	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_12).....	2283
3.887	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_13).....	2284
3.888	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_14).....	2285
3.889	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_15).....	2286
3.890	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_16).....	2287
3.891	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_17).....	2288
3.892	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_18).....	2289
3.893	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_19).....	2290
3.894	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_20).....	2291
3.895	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_21).....	2292
3.896	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_22).....	2293
3.897	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_23).....	2294
3.898	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_24).....	2295
3.899	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_25).....	2296
3.900	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_26).....	2297
3.901	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_27).....	2299
3.902	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_28).....	2300
3.903	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_29).....	2301
3.904	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_30).....	2302
3.905	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_31).....	2303
3.906	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_32).....	2304
3.907	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_33).....	2305
3.908	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_34).....	2307
3.909	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_35).....	2308
3.910	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_36).....	2309
3.911	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_37).....	2310
3.912	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_38).....	2311
3.913	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_39).....	2312
3.914	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_40).....	2314

3.915	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_41).....	2315
3.916	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_42).....	2316
3.917	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_43).....	2317
3.918	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_44).....	2318
3.919	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_45).....	2319
3.920	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_46).....	2321
3.921	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_47).....	2322
3.922	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_48).....	2323
3.923	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_49).....	2324
3.924	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_50).....	2325
3.925	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_51).....	2326
3.926	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_52).....	2327
3.927	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_53).....	2329
3.928	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_54).....	2330
3.929	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_55).....	2331
3.930	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_56).....	2332
3.931	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_57).....	2333
3.932	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_58).....	2334
3.933	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_59).....	2335
3.934	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_60).....	2336
3.935	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_61).....	2337
3.936	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_62).....	2339
3.937	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_63).....	2340
3.938	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_64).....	2341
3.939	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_65).....	2342
3.940	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_66).....	2344
3.941	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_67).....	2345
3.942	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_68).....	2346
3.943	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_69).....	2347
3.944	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_70).....	2348
3.945	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_71).....	2350
3.946	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_72).....	2351
3.947	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_73).....	2352
3.948	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_74).....	2353
3.949	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_75).....	2354
3.950	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_76).....	2355
3.951	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_77).....	2356
3.952	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_78).....	2357
3.953	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_79).....	2359
3.954	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_80).....	2360
3.955	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_81).....	2361
3.956	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_82).....	2362

3.957	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_83).....	2363
3.958	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_84).....	2364
3.959	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_85).....	2365
3.960	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_86).....	2366
3.961	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_87).....	2367
3.962	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_88).....	2369
3.963	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_89).....	2370
3.964	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_90).....	2371
3.965	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_91).....	2372
3.966	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_92).....	2373
3.967	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_93).....	2375
3.968	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_94).....	2376
3.969	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_95).....	2377
3.970	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_96).....	2378
3.971	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_97).....	2379
3.972	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_98).....	2381
3.973	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_99).....	2382
3.974	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_100).....	2383
3.975	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_101).....	2384
3.976	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_102).....	2385
3.977	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_103).....	2386
3.978	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_104).....	2387
3.979	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_105).....	2388
3.980	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_106).....	2390
3.981	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_107).....	2391
3.982	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_108).....	2392
3.983	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_109).....	2393
3.984	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_110).....	2394
3.985	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_111).....	2395
3.986	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_112).....	2396
3.987	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_113).....	2397
3.988	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_114).....	2399
3.989	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_115).....	2400
3.990	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_116).....	2401
3.991	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_117).....	2402
3.992	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_118).....	2403
3.993	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_119).....	2404
3.994	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_120).....	2405
3.995	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_121).....	2407
3.996	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_122).....	2408
3.997	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_123).....	2409
3.998	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_124).....	2410

3.999	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_125).....	2411
3.1000	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_126).....	2413
3.1001	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_127).....	2414
3.1002	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_128).....	2415
3.1003	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_129).....	2416
3.1004	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_130).....	2417
3.1005	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_131).....	2418
3.1006	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_132).....	2419
3.1007	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_133).....	2421
3.1008	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_134).....	2422
3.1009	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_135).....	2423
3.1010	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_136).....	2424
3.1011	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_137).....	2425
3.1012	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_138).....	2426
3.1013	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_139).....	2427
3.1014	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_140).....	2428
3.1015	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_141).....	2430
3.1016	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_142).....	2431
3.1017	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_143).....	2432
3.1018	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_144).....	2433
3.1019	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_145).....	2434
3.1020	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_146).....	2435
3.1021	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_147).....	2436
3.1022	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_148).....	2438
3.1023	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_149).....	2439
3.1024	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_150).....	2440
3.1025	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_151).....	2441
3.1026	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_152).....	2442
3.1027	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_153).....	2443
3.1028	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_154).....	2445
3.1029	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_155).....	2446
3.1030	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_156).....	2447
3.1031	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_157).....	2448
3.1032	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_158).....	2449
3.1033	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_159).....	2450
3.1034	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_160).....	2452
3.1035	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_161).....	2453
3.1036	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_162).....	2454
3.1037	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_163).....	2455
3.1038	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_164).....	2456
3.1039	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_165).....	2457
3.1040	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_166).....	2458

3.1041	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_167).....	2459
3.1042	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_168).....	2460
3.1043	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_169).....	2461
3.1044	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_170).....	2462
3.1045	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_171).....	2463
3.1046	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_172).....	2464
3.1047	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_173).....	2465
3.1048	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_174).....	2466
3.1049	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_175).....	2468
3.1050	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_176).....	2469
3.1051	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_177).....	2470
3.1052	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_178).....	2471
3.1053	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_179).....	2472
3.1054	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_180).....	2473
3.1055	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_181).....	2474
3.1056	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_182).....	2475
3.1057	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_183).....	2476
3.1058	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_184).....	2477
3.1059	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_185).....	2478
3.1060	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_186).....	2479
3.1061	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_187).....	2480
3.1062	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_188).....	2481
3.1063	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_189).....	2482
3.1064	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_190).....	2483
3.1065	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_191).....	2484
3.1066	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_192).....	2485
3.1067	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_193).....	2486
3.1068	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_194).....	2487
3.1069	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_195).....	2488
3.1070	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_196).....	2489
3.1071	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_197).....	2490
3.1072	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_198).....	2491
3.1073	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_199).....	2492
3.1074	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_200).....	2494
3.1075	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_201).....	2495
3.1076	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_202).....	2496
3.1077	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_203).....	2497
3.1078	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_204).....	2498
3.1079	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_205).....	2499
3.1080	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_206).....	2500
3.1081	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_207).....	2501
3.1082	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_208).....	2502

3.1083	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_209).....	2503
3.1084	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_210).....	2504
3.1085	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_211).....	2505
3.1086	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_212).....	2506
3.1087	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_213).....	2507
3.1088	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_214).....	2508
3.1089	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_215).....	2509
3.1090	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_216).....	2510
3.1091	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_217).....	2512
3.1092	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_218).....	2513
3.1093	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_219).....	2514
3.1094	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_220).....	2515
3.1095	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_221).....	2516
3.1096	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_222).....	2517
3.1097	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_223).....	2518
3.1098	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_224).....	2519
3.1099	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_225).....	2520
3.1100	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_226).....	2521
3.1101	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_227).....	2522
3.1102	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_228).....	2523
3.1103	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_229).....	2524
3.1104	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_230).....	2525
3.1105	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_231).....	2526
3.1106	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_232).....	2527
3.1107	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_233).....	2528
3.1108	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_234).....	2529
3.1109	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_235).....	2530
3.1110	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_236).....	2531
3.1111	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_237).....	2532
3.1112	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_238).....	2533
3.1113	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_239).....	2534
3.1114	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_240).....	2535
3.1115	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_241).....	2536
3.1116	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_242).....	2538
3.1117	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_243).....	2539
3.1118	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_244).....	2540
3.1119	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_245).....	2541
3.1120	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_246).....	2542
3.1121	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_247).....	2543
3.1122	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_248).....	2544
3.1123	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_249).....	2545
3.1124	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_250).....	2546

3.1125	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_251).....	2547
3.1126	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_252).....	2548
3.1127	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_253).....	2549
3.1128	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_254).....	2550
3.1129	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_255).....	2551
3.1130	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_256).....	2552
3.1131	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_257).....	2553
3.1132	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_258).....	2554
3.1133	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_259).....	2555
3.1134	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_260).....	2556
3.1135	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_261).....	2557
3.1136	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_262).....	2558
3.1137	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_263).....	2560
3.1138	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_264).....	2561
3.1139	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_265).....	2562
3.1140	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_266).....	2564
3.1141	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_267).....	2565
3.1142	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_268).....	2566
3.1143	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_269).....	2567
3.1144	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_270).....	2568
3.1145	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_271).....	2569
3.1146	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_272).....	2570
3.1147	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_273).....	2571
3.1148	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_274).....	2572
3.1149	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_275).....	2573
3.1150	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_276).....	2574
3.1151	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_277).....	2575
3.1152	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_278).....	2576
3.1153	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_279).....	2577
3.1154	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_280).....	2578
3.1155	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_281).....	2579
3.1156	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_282).....	2580
3.1157	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_283).....	2581
3.1158	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_284).....	2582
3.1159	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_285).....	2584
3.1160	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_286).....	2585
3.1161	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_287).....	2586
3.1162	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_288).....	2587
3.1163	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_289).....	2588
3.1164	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_290).....	2589
3.1165	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_291).....	2590
3.1166	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_292).....	2591

3.1167	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_293).....	2592
3.1168	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_294).....	2593
3.1169	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_295).....	2594
3.1170	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_296).....	2595
3.1171	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_297).....	2596
3.1172	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_298).....	2597
3.1173	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_299).....	2598
3.1174	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_300).....	2599
3.1175	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_301).....	2600
3.1176	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_302).....	2601
3.1177	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_303).....	2602
3.1178	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_304).....	2603
3.1179	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_305).....	2604
3.1180	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_306).....	2605
3.1181	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_307).....	2606
3.1182	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_308).....	2607
3.1183	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_309).....	2608
3.1184	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_310).....	2609
3.1185	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_311).....	2610
3.1186	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_312).....	2611
3.1187	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_313).....	2612
3.1188	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_314).....	2613
3.1189	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_315).....	2614
3.1190	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_316).....	2615
3.1191	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_317).....	2616
3.1192	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_318).....	2617
3.1193	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_319).....	2618
3.1194	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_320).....	2619
3.1195	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_321).....	2620
3.1196	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_322).....	2621
3.1197	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_323).....	2622
3.1198	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_324).....	2624
3.1199	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_325).....	2625
3.1200	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_326).....	2626
3.1201	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_327).....	2627
3.1202	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_328).....	2628
3.1203	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_329).....	2629
3.1204	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_330).....	2630
3.1205	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_331).....	2631
3.1206	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_332).....	2632
3.1207	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_333).....	2633
3.1208	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_334).....	2634

3.1209	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_335).....	2635
3.1210	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_336).....	2636
3.1211	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_337).....	2637
3.1212	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_338).....	2638
3.1213	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_339).....	2639
3.1214	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_340).....	2640
3.1215	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_341).....	2641
3.1216	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_342).....	2642
3.1217	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_343).....	2643
3.1218	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_344).....	2645
3.1219	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_345).....	2646
3.1220	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_346).....	2647
3.1221	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_347).....	2648
3.1222	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_348).....	2649
3.1223	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_349).....	2650
3.1224	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_350).....	2651
3.1225	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_351).....	2652
3.1226	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_352).....	2653
3.1227	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_353).....	2655
3.1228	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_354).....	2656
3.1229	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_355).....	2657
3.1230	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_356).....	2658
3.1231	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_357).....	2659
3.1232	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_358).....	2661
3.1233	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_359).....	2662
3.1234	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_360).....	2663
3.1235	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_361).....	2664
3.1236	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_362).....	2665
3.1237	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_363).....	2666
3.1238	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_364).....	2668
3.1239	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_365).....	2669
3.1240	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_366).....	2670
3.1241	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_367).....	2671
3.1242	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_368).....	2672
3.1243	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_369).....	2673
3.1244	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_370).....	2674
3.1245	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_371).....	2675
3.1246	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_372).....	2676
3.1247	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_373).....	2678
3.1248	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_374).....	2679
3.1249	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_375).....	2680
3.1250	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_376).....	2681

3.1251	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_377).....	2682
3.1252	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_378).....	2683
3.1253	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_379).....	2684
3.1254	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_380).....	2686
3.1255	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_381).....	2687
3.1256	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_382).....	2688
3.1257	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_383).....	2689
3.1258	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_384).....	2690
3.1259	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_385).....	2691
3.1260	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_386).....	2692
3.1261	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_387).....	2693
3.1262	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_388).....	2694
3.1263	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_389).....	2696
3.1264	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_390).....	2697
3.1265	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_391).....	2698
3.1266	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_392).....	2699
3.1267	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_393).....	2700
3.1268	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_394).....	2702
3.1269	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_395).....	2703
3.1270	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_396).....	2704
3.1271	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_397).....	2705
3.1272	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_398).....	2706
3.1273	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_399).....	2708
3.1274	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_400).....	2709
3.1275	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_401).....	2710
3.1276	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_402).....	2711
3.1277	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_403).....	2712
3.1278	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_404).....	2713
3.1279	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_405).....	2714
3.1280	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_406).....	2715
3.1281	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_407).....	2716
3.1282	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_408).....	2717
3.1283	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_409).....	2719
3.1284	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_410).....	2720
3.1285	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_411).....	2721
3.1286	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_412).....	2722
3.1287	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_413).....	2723
3.1288	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_414).....	2724
3.1289	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_415).....	2725
3.1290	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_416).....	2726
3.1291	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_417).....	2727
3.1292	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_418).....	2729

3.1293	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_419).....	2730
3.1294	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_420).....	2731
3.1295	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_421).....	2732
3.1296	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_422).....	2733
3.1297	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_423).....	2735
3.1298	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_424).....	2736
3.1299	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_425).....	2737
3.1300	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_426).....	2738
3.1301	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_427).....	2739
3.1302	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_428).....	2740
3.1303	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_429).....	2741
3.1304	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_430).....	2743
3.1305	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_431).....	2744
3.1306	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_432).....	2745
3.1307	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_433).....	2746
3.1308	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_434).....	2747
3.1309	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_435).....	2748
3.1310	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_436).....	2749
3.1311	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_437).....	2750
3.1312	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_438).....	2752
3.1313	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_439).....	2753
3.1314	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_440).....	2754
3.1315	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_441).....	2755
3.1316	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_442).....	2756
3.1317	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_443).....	2757
3.1318	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_444).....	2758
3.1319	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_445).....	2759
3.1320	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_446).....	2761
3.1321	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_447).....	2762
3.1322	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_448).....	2763
3.1323	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_449).....	2764
3.1324	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_450).....	2765
3.1325	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_451).....	2766
3.1326	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_452).....	2767
3.1327	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_453).....	2768
3.1328	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_454).....	2770
3.1329	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_455).....	2771
3.1330	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_456).....	2772
3.1331	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_457).....	2773
3.1332	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_458).....	2774
3.1333	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_459).....	2775
3.1334	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_460).....	2777

3.1335	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_461).....	2778
3.1336	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_462).....	2779
3.1337	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_463).....	2780
3.1338	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_464).....	2781
3.1339	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_465).....	2782
3.1340	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_466).....	2784
3.1341	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_467).....	2785
3.1342	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_468).....	2786
3.1343	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_469).....	2787
3.1344	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_470).....	2788
3.1345	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_471).....	2789
3.1346	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_472).....	2790
3.1347	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_473).....	2792
3.1348	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_474).....	2793
3.1349	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_475).....	2794
3.1350	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_476).....	2795
3.1351	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_477).....	2796
3.1352	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_478).....	2797
3.1353	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_479).....	2798
3.1354	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_480).....	2799
3.1355	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_481).....	2800
3.1356	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_482).....	2802
3.1357	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_483).....	2803
3.1358	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_484).....	2804
3.1359	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_485).....	2805
3.1360	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_486).....	2806
3.1361	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_487).....	2807
3.1362	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_488).....	2808
3.1363	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_489).....	2810
3.1364	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_490).....	2811
3.1365	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_491).....	2812
3.1366	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_492).....	2813
3.1367	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_493).....	2814
3.1368	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_494).....	2815
3.1369	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_495).....	2816
3.1370	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_496).....	2818
3.1371	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_497).....	2819
3.1372	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_498).....	2820
3.1373	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_499).....	2821
3.1374	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_500).....	2822
3.1375	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_501).....	2824
3.1376	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_502).....	2825

3.1377	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_503).....	2826
3.1378	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_504).....	2827
3.1379	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_505).....	2828
3.1380	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_506).....	2829
3.1381	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_507).....	2830
3.1382	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_508).....	2831
3.1383	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_509).....	2832
3.1384	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_510).....	2834
3.1385	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_511).....	2835
3.1386	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_512).....	2836
3.1387	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_513).....	2837
3.1388	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_514).....	2838
3.1389	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_515).....	2839
3.1390	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_516).....	2840
3.1391	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_517).....	2841
3.1392	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_518).....	2842
3.1393	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_519).....	2844
3.1394	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_520).....	2845
3.1395	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_521).....	2846
3.1396	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_522).....	2847
3.1397	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_523).....	2848
3.1398	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_524).....	2849
3.1399	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_525).....	2850
3.1400	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_526).....	2852
3.1401	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_527).....	2853
3.1402	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_528).....	2854
3.1403	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_529).....	2855
3.1404	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_530).....	2856
3.1405	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_531).....	2857
3.1406	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_532).....	2858
3.1407	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_533).....	2860
3.1408	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_534).....	2861
3.1409	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_535).....	2862
3.1410	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_536).....	2863
3.1411	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_537).....	2864
3.1412	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_538).....	2866
3.1413	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_539).....	2867
3.1414	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_540).....	2868
3.1415	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_541).....	2869
3.1416	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_542).....	2870
3.1417	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_543).....	2871
3.1418	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_544).....	2872

3.1419	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_545).....	2873
3.1420	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_546).....	2874
3.1421	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_547).....	2876
3.1422	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_548).....	2877
3.1423	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_549).....	2878
3.1424	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_550).....	2879
3.1425	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_551).....	2880
3.1426	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_552).....	2881
3.1427	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_553).....	2882
3.1428	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_554).....	2883
3.1429	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_555).....	2884
3.1430	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_556).....	2886
3.1431	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_557).....	2887
3.1432	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_558).....	2888
3.1433	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_559).....	2889
3.1434	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_560).....	2890
3.1435	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_561).....	2891
3.1436	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_562).....	2892
3.1437	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_563).....	2894
3.1438	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_564).....	2895
3.1439	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_565).....	2896
3.1440	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_566).....	2897
3.1441	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_567).....	2898
3.1442	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_568).....	2899
3.1443	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_569).....	2901
3.1444	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_570).....	2902
3.1445	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_571).....	2903
3.1446	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_572).....	2904
3.1447	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_573).....	2905
3.1448	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_574).....	2907
3.1449	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_575).....	2908
3.1450	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_576).....	2909
3.1451	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_577).....	2910
3.1452	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_578).....	2911
3.1453	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_579).....	2912
3.1454	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_580).....	2913
3.1455	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_581).....	2914
3.1456	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_582).....	2915
3.1457	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_583).....	2916
3.1458	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_584).....	2918
3.1459	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_585).....	2919
3.1460	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_586).....	2920

3.1461	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_587).....	2921
3.1462	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_588).....	2922
3.1463	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_589).....	2923
3.1464	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_590).....	2924
3.1465	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_591).....	2925
3.1466	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_592).....	2926
3.1467	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_593).....	2928
3.1468	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_594).....	2929
3.1469	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_595).....	2930
3.1470	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_596).....	2931
3.1471	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_597).....	2932
3.1472	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_598).....	2933
3.1473	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_599).....	2934
3.1474	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_600).....	2936
3.1475	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_601).....	2937
3.1476	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_602).....	2938
3.1477	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_603).....	2939
3.1478	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_604).....	2940
3.1479	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_605).....	2941
3.1480	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_606).....	2942
3.1481	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_607).....	2944
3.1482	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_608).....	2945
3.1483	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_609).....	2946
3.1484	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_610).....	2947
3.1485	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_611).....	2948
3.1486	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_612).....	2949
3.1487	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_613).....	2950
3.1488	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_614).....	2951
3.1489	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_615).....	2953
3.1490	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_616).....	2954
3.1491	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_617).....	2955
3.1492	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_618).....	2956
3.1493	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_619).....	2957
3.1494	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_620).....	2958
3.1495	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_621).....	2959
3.1496	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_622).....	2960
3.1497	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_623).....	2962
3.1498	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_624).....	2963
3.1499	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_625).....	2964
3.1500	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_626).....	2965
3.1501	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_627).....	2966
3.1502	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_628).....	2967

3.1503	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_629).....	2968
3.1504	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_630).....	2969
3.1505	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_631).....	2971
3.1506	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_632).....	2972
3.1507	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_633).....	2973
3.1508	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_634).....	2974
3.1509	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_635).....	2975
3.1510	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_636).....	2976
3.1511	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_637).....	2977
3.1512	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_638).....	2979
3.1513	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_639).....	2980
3.1514	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_640).....	2981
3.1515	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_641).....	2982
3.1516	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_642).....	2983
3.1517	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_643).....	2984
3.1518	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_644).....	2985
3.1519	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_645).....	2986
3.1520	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_646).....	2988
3.1521	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_647).....	2989
3.1522	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_648).....	2990
3.1523	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_649).....	2991
3.1524	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_650).....	2992
3.1525	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_651).....	2993
3.1526	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_652).....	2994
3.1527	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_653).....	2995
3.1528	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_654).....	2997
3.1529	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_655).....	2998
3.1530	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_656).....	2999
3.1531	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_657).....	3000
3.1532	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_658).....	3001
3.1533	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_659).....	3002
3.1534	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_660).....	3003
3.1535	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_661).....	3004
3.1536	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_662).....	3006
3.1537	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_663).....	3007
3.1538	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_664).....	3008
3.1539	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_665).....	3009
3.1540	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_666).....	3010
3.1541	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_667).....	3011
3.1542	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_668).....	3012
3.1543	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_669).....	3014
3.1544	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_670).....	3015

3.1545	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_671).....	3016
3.1546	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_672).....	3017
3.1547	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_673).....	3018
3.1548	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_674).....	3019
3.1549	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_675).....	3021
3.1550	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_676).....	3022
3.1551	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_677).....	3023
3.1552	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_678).....	3024
3.1553	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_679).....	3025
3.1554	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_680).....	3026
3.1555	Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_681).....	3027
3.1556	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_1).....	3029
3.1557	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_2).....	3030
3.1558	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_3).....	3031
3.1559	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_4).....	3032
3.1560	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_5).....	3033
3.1561	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_6).....	3034
3.1562	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_7).....	3035
3.1563	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_8).....	3036
3.1564	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_9).....	3037
3.1565	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_10).....	3038
3.1566	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_11).....	3039
3.1567	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_12).....	3040
3.1568	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_13).....	3041
3.1569	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_14).....	3043
3.1570	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_15).....	3044
3.1571	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_16).....	3045
3.1572	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_17).....	3046
3.1573	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_18).....	3047
3.1574	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_19).....	3048
3.1575	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_20).....	3050
3.1576	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_21).....	3051
3.1577	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_22).....	3052
3.1578	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_23).....	3053
3.1579	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_24).....	3054
3.1580	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_25).....	3055
3.1581	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_26).....	3056
3.1582	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_27).....	3057
3.1583	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_28).....	3058
3.1584	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_29).....	3060
3.1585	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_30).....	3061
3.1586	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_31).....	3062

3.1587	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_32).....	3063
3.1588	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_33).....	3064
3.1589	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_34).....	3066
3.1590	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_35).....	3067
3.1591	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_36).....	3068
3.1592	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_37).....	3069
3.1593	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_38).....	3070
3.1594	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_39).....	3071
3.1595	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_40).....	3072
3.1596	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_41).....	3073
3.1597	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_2_42).....	3074
3.1598	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_2_43).....	3075
3.1599	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_2_44).....	3077
3.1600	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_2_45).....	3078
3.1601	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_2_46).....	3079
3.1602	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_2_47).....	3080
3.1603	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_2_48).....	3081
3.1604	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_2_49).....	3082
3.1605	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_2_50).....	3083
3.1606	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_2_51).....	3084
3.1607	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_2_52).....	3085
3.1608	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_2_53).....	3086
3.1609	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_54).....	3087
3.1610	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_55).....	3088
3.1611	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_56).....	3089
3.1612	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_57).....	3091
3.1613	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_58).....	3092
3.1614	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_59).....	3093
3.1615	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_60).....	3094
3.1616	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_61).....	3095
3.1617	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_62).....	3096
3.1618	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_63).....	3097
3.1619	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_64).....	3098
3.1620	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_65).....	3099
3.1621	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_66).....	3100
3.1622	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_67).....	3101
3.1623	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_68).....	3103
3.1624	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_69).....	3104
3.1625	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_70).....	3105
3.1626	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_71).....	3106
3.1627	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_72).....	3107
3.1628	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_73).....	3108

3.1629	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_74).....	3109
3.1630	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_75).....	3110
3.1631	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_76).....	3111
3.1632	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_77).....	3112
3.1633	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_78).....	3113
3.1634	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_79).....	3114
3.1635	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_80).....	3115
3.1636	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_81).....	3116
3.1637	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_82).....	3117
3.1638	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_83).....	3118
3.1639	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_84).....	3119
3.1640	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_85).....	3120
3.1641	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_86).....	3121
3.1642	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_87).....	3123
3.1643	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_88).....	3124
3.1644	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_89).....	3125
3.1645	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_90).....	3126
3.1646	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_91).....	3127
3.1647	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_92).....	3128
3.1648	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_93).....	3129
3.1649	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_94).....	3130
3.1650	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_95).....	3131
3.1651	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_96).....	3132
3.1652	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_97).....	3133
3.1653	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_98).....	3134
3.1654	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_99).....	3135
3.1655	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_100).....	3136
3.1656	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_101).....	3137
3.1657	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_102).....	3138
3.1658	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_103).....	3139
3.1659	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_104).....	3141
3.1660	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_105).....	3142
3.1661	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_106).....	3143
3.1662	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_107).....	3144
3.1663	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_108).....	3145
3.1664	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_109).....	3146
3.1665	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_110).....	3147
3.1666	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_111).....	3148
3.1667	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_112).....	3149
3.1668	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_113).....	3150
3.1669	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_114).....	3151
3.1670	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_115).....	3152

3.1671	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_116).....	3153
3.1672	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_117).....	3154
3.1673	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_118).....	3155
3.1674	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_119).....	3156
3.1675	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_120).....	3157
3.1676	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_121).....	3158
3.1677	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_122).....	3159
3.1678	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_123).....	3160
3.1679	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_124).....	3161
3.1680	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_125).....	3162
3.1681	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_126).....	3163
3.1682	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_127).....	3164
3.1683	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_128).....	3165
3.1684	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_129).....	3166
3.1685	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_130).....	3167
3.1686	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_131).....	3168
3.1687	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_1).....	3169
3.1688	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_2).....	3170
3.1689	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_3).....	3171
3.1690	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_4).....	3172
3.1691	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_5).....	3173
3.1692	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_6).....	3174
3.1693	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_7).....	3175
3.1694	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_8).....	3176
3.1695	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_9).....	3178
3.1696	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_10).....	3179
3.1697	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_11).....	3180
3.1698	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_12).....	3181
3.1699	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_13).....	3182
3.1700	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_14).....	3183
3.1701	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_15).....	3184
3.1702	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_16).....	3186
3.1703	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_17).....	3187
3.1704	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_18).....	3188
3.1705	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_19).....	3189
3.1706	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_20).....	3190
3.1707	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_21).....	3191
3.1708	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_22).....	3192
3.1709	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_23).....	3193
3.1710	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_24).....	3194
3.1711	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_25).....	3196
3.1712	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_26).....	3197

3.1713	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_27).....	3198
3.1714	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_28).....	3199
3.1715	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_29).....	3200
3.1716	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_30).....	3201
3.1717	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_31).....	3203
3.1718	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_32).....	3204
3.1719	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_33).....	3205
3.1720	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_34).....	3206
3.1721	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_35).....	3207
3.1722	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_36).....	3209
3.1723	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_37).....	3210
3.1724	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_38).....	3211
3.1725	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_39).....	3212
3.1726	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_8_40).....	3213
3.1727	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_8_41).....	3214
3.1728	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_8_42).....	3215
3.1729	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_8_43).....	3216
3.1730	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_8_44).....	3217
3.1731	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_8_45).....	3218
3.1732	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_8_46).....	3219
3.1733	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_8_47).....	3220
3.1734	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_8_48).....	3222
3.1735	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_8_49).....	3223
3.1736	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_8_50).....	3224
3.1737	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_8_51).....	3225
3.1738	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_52).....	3226
3.1739	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_53).....	3227
3.1740	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_54).....	3228
3.1741	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_55).....	3229
3.1742	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_56).....	3230
3.1743	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_57).....	3231
3.1744	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_58).....	3232
3.1745	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_59).....	3233
3.1746	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_60).....	3235
3.1747	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_61).....	3236
3.1748	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_62).....	3237
3.1749	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_63).....	3238
3.1750	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_64).....	3239
3.1751	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_65).....	3240
3.1752	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_66).....	3241
3.1753	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_67).....	3242
3.1754	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_68).....	3243

3.1755	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_69).....	3245
3.1756	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_70).....	3246
3.1757	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_71).....	3247
3.1758	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_72).....	3248
3.1759	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_73).....	3249
3.1760	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_74).....	3250
3.1761	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_75).....	3251
3.1762	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_76).....	3252
3.1763	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_77).....	3253
3.1764	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_78).....	3254
3.1765	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_79).....	3255
3.1766	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_80).....	3257
3.1767	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_81).....	3258
3.1768	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_82).....	3259
3.1769	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_83).....	3260
3.1770	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_84).....	3261
3.1771	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_85).....	3262
3.1772	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_86).....	3263
3.1773	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_87).....	3264
3.1774	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_88).....	3266
3.1775	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_89).....	3267
3.1776	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_90).....	3268
3.1777	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_91).....	3269
3.1778	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_92).....	3270
3.1779	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_93).....	3271
3.1780	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_94).....	3272
3.1781	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_95).....	3273
3.1782	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_96).....	3274
3.1783	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_97).....	3276
3.1784	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_98).....	3277
3.1785	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_99).....	3278
3.1786	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_100).....	3279
3.1787	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_101).....	3280
3.1788	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_102).....	3281
3.1789	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_103).....	3282
3.1790	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_104).....	3283
3.1791	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_105).....	3284
3.1792	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_106).....	3285
3.1793	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_107).....	3286
3.1794	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_108).....	3287
3.1795	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_109).....	3288
3.1796	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_110).....	3289

3.1797	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_111).....	3290
3.1798	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_112).....	3291
3.1799	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_113).....	3292
3.1800	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_114).....	3293
3.1801	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_115).....	3294
3.1802	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_116).....	3295
3.1803	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_117).....	3296
3.1804	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_118).....	3297
3.1805	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_119).....	3298
3.1806	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_120).....	3299
3.1807	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_121).....	3300
3.1808	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_122).....	3301
3.1809	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_123).....	3302
3.1810	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_124).....	3303
3.1811	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_125).....	3304
3.1812	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_126).....	3305
3.1813	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_127).....	3306
3.1814	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_128).....	3307
3.1815	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_129).....	3308
3.1816	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_130).....	3309
3.1817	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_13_1).....	3310
3.1818	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_13_2).....	3311
3.1819	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_14_3).....	3312
3.1820	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_15_4).....	3313
3.1821	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_15_5).....	3314
3.1822	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_15_6).....	3315
3.1823	Testfall: Datei- und Objektsystem (TC_Funktion_EFO_16_7).....	3316
3.1824	Testfall: Unterstützung CA (TC_Funktion_CAF_1).....	3317
3.1825	Testfall: Unterstützung CA (TC_Funktion_CAF_2).....	3318
3.1826	Testfall: Protokolle (TC_Funktion_P_1).....	3319
4	Usecase-Tests.....	3320
4.1	Testfall: VI_01_01.....	3320
4.2	Testfall: VI_02_01a.....	3321
4.3	Testfall: VI_02_01b.....	3323
4.4	Testfall: VI_02_01c.....	3324
4.5	Testfall: VI_02_01d.....	3326
4.6	Testfall: VI_02_02a.....	3327
4.7	Testfall: VI_02_03.....	3329
4.8	Testfall: VI_02_04.....	3331
4.9	Testfall: VI_02_05.....	3332
4.10	Testfall: VI_02_06.....	3335
4.11	Testfall: VI_02_07.....	3337

4.12	Testfall: VI_02_08.....	3340
4.13	Testfall: VI_02_09.....	3343
4.14	Testfall: VI_02_10.....	3345
4.15	Testfall: VI_02_11a.....	3347
4.16	Testfall: VI_02_11b.....	3349
4.17	Testfall: VI_02_12a.....	3351
4.18	Testfall: VI_02_12b.....	3353
4.19	Testfall: VI_02_13a.....	3354
4.20	Testfall: VI_02_13b.....	3356
4.21	Testfall: VI_02_14a.....	3357
4.22	Testfall: VI_02_14b.....	3359
4.23	Testfall: VI_03_01a.....	3361
4.24	Testfall: VI_03_01b.....	3363
4.25	Testfall: VI_03_02.....	3365
4.26	Testfall: VI_03_03.....	3367
4.27	Testfall: VI_03_04.....	3369
4.28	Testfall: VI_03_05a.....	3372
4.29	Testfall: VI_03_05b.....	3374
4.30	Testfall: VI_04_01.....	3376
4.31	Testfall: VI_04_02a.....	3378
4.32	Testfall: VI_04_02b.....	3379
4.33	Testfall: VI_05_01.....	3381
4.34	Testfall: VI_05_02.....	3383
4.35	Testfall: VI_05_03.....	3385
4.36	Testfall: VI_05_04.....	3386
4.37	Testfall: VI_05_05.....	3388
4.38	Testfall: PN_01_01.....	3390
4.39	Testfall: PN_02_01a.....	3392
4.40	Testfall: PN_02_01b.....	3394
4.41	Testfall: PN_02_02a.....	3395
4.42	Testfall: PN_02_02b.....	3397
4.43	Testfall: PN_02_03a.....	3399
4.44	Testfall: PN_02_03b.....	3401
4.45	Testfall: PN_03_01.....	3403
4.46	Testfall: PN_03_02.....	3405
4.47	Testfall: PN_03_03.....	3407
4.48	Testfall: PN_03_04a.....	3409
4.49	Testfall: PN_03_04b.....	3411
4.50	Testfall: PN_03_05a.....	3412
4.51	Testfall: PN_03_05b.....	3414
4.52	Testfall: PN_04_01.....	3416
4.53	Testfall: PN_04_02.....	3418

4.54	Testfall: PN_04_03.....	3421
4.55	Testfall: PN_04_04.....	3422
4.56	Testfall: PN_04_05.....	3426
4.57	Testfall: PN_04_06.....	3428
4.58	Testfall: PN_04_07.....	3430
4.59	Testfall: PN_04_08.....	3432
4.60	Testfall: PN_04_09a.....	3434
4.61	Testfall: PN_04_10.....	3437
4.62	Testfall: PN_04_11.....	3439
4.63	Testfall: PN_04_12.....	3442
4.64	Testfall: PN_04_13.....	3446
4.65	Testfall: PN_04_14a.....	3448
4.66	Testfall: PN_04_14b.....	3451
4.67	Testfall: PN_04_15a.....	3453
4.68	Testfall: PN_04_15b.....	3455
4.69	Testfall: PN_04_16a.....	3457
4.70	Testfall: PN_04_16b.....	3458
4.71	Testfall: PN_04_16c.....	3460
4.72	Testfall: PN_04_16d.....	3462
4.73	Testfall: PN_04_17.....	3463
4.74	Testfall: PN_04_18a.....	3465
4.75	Testfall: PN_04_19a.....	3467
4.76	Testfall: PN_04_20a.....	3469
4.77	Testfall: PN_04_21a.....	3471
4.78	Testfall: PN_04_21b.....	3473
4.79	Testfall: PN_04_22.....	3475
4.80	Testfall: PN_04_23.....	3477
4.81	Testfall: PN_05_01.....	3479
4.82	Testfall: PN_05_02.....	3480
4.83	Testfall: PN_05_03.....	3483
4.84	Testfall: PN_05_04a.....	3485
4.85	Testfall: PN_05_04b.....	3487
4.86	Testfall: PN_05_05.....	3489
4.87	Testfall: PN_05_06.....	3493
4.88	Testfall: PN_05_07.....	3496
4.89	Testfall: PN_05_08a.....	3499
4.90	Testfall: PN_05_08b.....	3502
4.91	Testfall: PN_05_09.....	3505
4.92	Testfall: PN_05_10.....	3506
4.93	Testfall: PN_05_11.....	3508
	Literaturverzeichnis.....	3511

1 Einleitung

Das Smart Meter Gateway (SMGW) nach der Technischen Richtlinie [BSI TR-03109-1] stellt die zentrale Kommunikationseinheit in der Infrastruktur eines elektronischen Messsystems dar. Das SMGW kommuniziert im lokalen Bereich beim Endkunden mit elektronischen Zählern des Local Metrological Network (LMN) und mit Geräten aus dem Home Area Network (HAN) und im Wide Area Network (WAN) mit autorisierten Marktteilnehmern. Außerdem ermöglicht das SMGW die Verbindungsaufnahme von lokalen Geräten des HAN über das WAN mit autorisierten Marktteilnehmern.

Zur Erfüllung der dazu benötigten kryptographischen Funktionen bedient sich das SMGW eines Smartmeter-Sicherheitsmoduls, das die kryptographische Identität des SMGW sicherstellt und als Service Provider für kryptographische Operationen dient. Die technische Spezifikation dieses Sicherheitsmoduls ist Gegenstand der Technischen Richtlinie [BSI TR-03109-2], die die grundsätzliche Konzeption des Sicherheitsmoduls beschreibt sowie die vom Sicherheitsmodul bereitgestellten Funktionalitäten, die vom Sicherheitsmodul angebotenen Kommandos, das vom Sicherheitsmodul verwaltete System von Ordnern, Datenfeldern, Key- und PIN-Objekten und die vom Sicherheitsmodul durchgesetzte Zugriffsregelpolitik definiert.

Smartmeter-Sicherheitsmodule, im folgenden kurz als Sicherheitsmodule bezeichnet, unterliegen einer CC-Sicherheitszertifizierung unter Verwendung des Protection Profiles [PP-0077].

Das vorliegende Dokument „Testdetailspezifikation für das Sicherheitsmodul nach BSI TR-03109-2“ bildet den dritten von insgesamt drei Teilen der „Testspezifikation zur Prüfung des Sicherheitsmoduls nach BSI TR-03109-2“ ([BSI TR-03109-TS-2]). Es dient der Detailbeschreibung von Tests zur Überprüfung des Sicherheitsmoduls.

Die „Testspezifikation zur Prüfung des Sicherheitsmoduls nach BSI TR-03109-2“ ([BSI TR-03109-TS-2]), im Folgenden kurz als Testspezifikation bezeichnet, gliedert sich insgesamt wie in folgender Abbildung dargestellt.

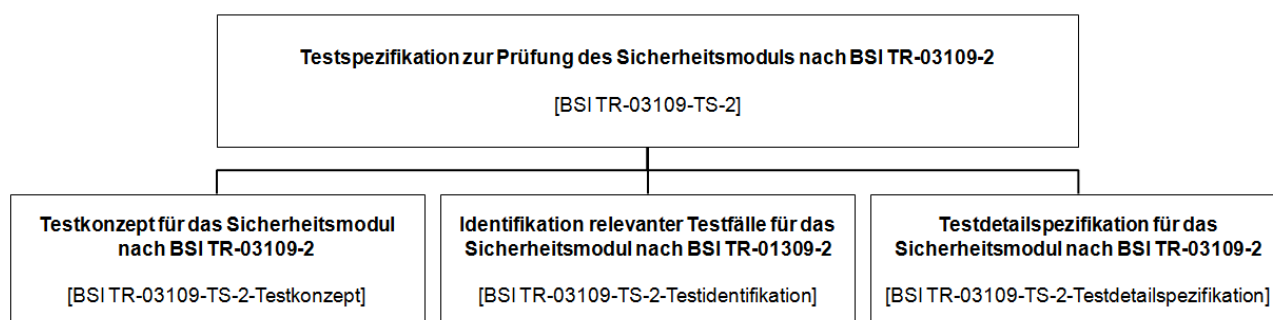


Abbildung 1: Aufbau der Testspezifikation

Die Testspezifikation dient dabei als Dachdokument für die im Folgenden dargestellten drei Dokumententeile:

1. Das Dokument „Testkonzept für das Sicherheitsmodul nach BSI TR-03109-2“ ([BSI TR-03109-TS-2-Testkonzept]), im Folgenden kurz als Testkonzept bezeichnet, dient der Beschreibung des grundsätzlichen Konzepts zur Durchführung von Konformitätsprüfungen des Sicherheitsmoduls gegen die funktionalen Vorgaben der Technischen Richtlinie [BSI TR-03109-2].

2. Das Dokument „Identifikation relevanter Testfälle für das Sicherheitsmodul nach BSI TR-01309-2“ ([BSI TR-03109-TS-2-Testidentifikation]), im Folgenden kurz als Testidentifikation bezeichnet, dient der Zusammenstellung und Beschreibung der für die Konformitätsprüfung eines Sicherheitsmoduls relevanten Testfälle.

Auf Basis des Testkonzepts für die Konformitätsprüfung eines Sicherheitsmoduls ([BSI TR-03109-TS-2-Testkonzept]) wird im Dokument Testidentifikation ([BSI TR-03109-TS-2-Testidentifikation]) genauer dargestellt, was bzw. welche Anforderungen an ein Sicherheitsmodul aus der Technischen Richtlinie [BSI TR-03109-2] getestet werden sollen.

Das Dokument Testidentifikation ([BSI TR-03109-TS-2-Testidentifikation]) zeigt somit insgesamt auf, was im Rahmen der TR-03109-TS-2 zu testen ist.

3. Im vorliegenden Dokument „Testdetailspezifikation für das Sicherheitsmodul nach BSI TR-03109-2“, im Folgenden kurz als Testdetailspezifikation bezeichnet, werden die im Dokument Testidentifikation ([BSI TR-03109-TS-2-Testidentifikation]) spezifizierten Testfälle für die Konformitätsprüfung eines Sicherheitsmoduls im Detail - sofern möglich - auf Implementierungsebene heruntergebrochen und in XML-Strukturen ([BSI TR-03109-TS-2-XML]) umgesetzt.

Das Dokument (bzw. seine XML-Datei [BSI TR-03109-TS-2-XML]) zeigt somit auf, wie die im Dokument Testidentifikation ([BSI TR-03109-TS-2-Testidentifikation]) identifizierten, generisch beschriebenen Testfälle konkret umzusetzen sind.

1.1 Zielsetzung

Das Dokument dient der detaillierten Beschreibung der Prüfungen und Tests zur Konformitätsprüfung des Sicherheitsmoduls gegen die funktionalen Vorgaben der Technischen Richtlinie [BSI TR-03109-2].

1.2 Bezugsdokumente

Das vorliegende Dokument beinhaltet die detaillierte Beschreibung der Prüfungen und Tests für gemäß der Technischen Richtlinie [BSI TR-03109-2] entwickelte Sicherheitsmodule.

Das Dokument bildet den dritten Teil von drei Dokumenten der „Testspezifikation zur Prüfung des Sicherheitsmoduls nach BSI TR-03109-2“ ([BSI TR-03109-TS-2]).

1.3 Nomenklatur

Nachfolgend findet sich eine Liste der Identifikatoren, die im Rahmen der Testfall-XML-Beschreibungen benutzt werden:

TC_[...]	Testfall	[...] ist eine Kurzbezeichnung, die Testfälle eindeutig unterscheidbar macht
CN-[...]	Vorbedingung/Nebenbedingung/Nachbedingung	[...] ist eine Kurzbezeichnung, die Bedingungen eindeutig unterscheidbar macht

CM- [...]	APDU-Kommando	[...] ist eine Kurzbezeichnung, die Kommandos eindeutig unterscheidbar macht
RS- [...]	Ergebnis	[...] ist eine Kurzbezeichnung, die Ergebnisse eindeutig unterscheidbar macht
VF- [...]	Verifikation	[...] ist eine Kurzbezeichnung, die Verifikationsschritte eindeutig unterscheidbar macht

Nachfolgend alle Platzhalter, die im Rahmen der Darstellung von APDUs benutzt werden:

LL	Hexadezimaler String von der Länge eines Bytes, der die Anzahl bzw. die Länge der nachfolgenden, im Data-Feld mit eckigen Klammern aufgeführten Bytes angibt.
XX	Hexadezimaler String mit einer Byte-Länge von 1.
XX...XX	Hexadezimaler String mit einer Mindest-Byte-Länge von 1. Die genaue Anzahl der Bytes ist kontextabhängig.

1.4 Versionshistorie

<i>Version</i>	<i>Datum</i>	<i>Änderungen</i>
1.0	06.03.2018	Finale Version / Erstausgabe

Tabelle 1: Versionshistorie

2 Kommando-Tests

Für alle Kommando-Testfälle gilt, dass ein durch "Memory Failure" angezeigter Schreibfehler während der Ausführung des Testfalls nicht auftreten darf.

2.1 Testfall: ACTIVATE FILE (TC_ACTIVATE_FILE_GF_1)

2.1.1 Informationen

ID	TC_ACTIVATE_FILE_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE FILE erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für ACTIVATE FILE zur Aktivierung eines DFs/EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.1.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.4

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.1.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-CURRENT_FILE-2	Das File ist ausgewählt

CN- OBJECT_TERMINATED-2	Objekt befindet sich nicht im Zustand "terminated"
CN- SECURITY_STATU S_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.1.4 APDU-Kommandos

ID: CM-ACTIVATE_FILE_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

2.1.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.1.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_FILE-1	Das entsprechende File ist auslesbar.

2.2 Testfall: ACTIVATE FILE (TC_ACTIVATE_FILE_FF_1)

2.2.1 Informationen

ID	TC_ACTIVATE_FILE_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE FILE nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für ACTIVATE FILE zur Aktivierung eines DFs/EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.

Klassifizierung	Fehlerfall-Test

2.2.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.4

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.2.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-CURRENT_FILE-2	Das File ist ausgewählt
CN-OBJECT_TERMINATED-2	Objekt befindet sich nicht im Zustand "terminated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.2.4 APDU-Kommandos

ID: CM-ACTIVATE_FILE_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

2.2.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.2.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_FILE-2	Das entsprechende File ist nicht auslesbar.

2.3 Testfall: ACTIVATE FILE (TC_ACTIVATE_FILE_FF_2)

2.3.1 Informationen

ID	TC_ACTIVATE_FILE_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE FILE nicht durchführen lässt, wenn das File vorher nicht selektiert wurde. Dazu wird eine Kommandonachricht für ACTIVATE FILE zur Aktivierung eines DFs/EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.3.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.4

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.3.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN- NO_CURRENT_FILE-1	Das File ist nicht ausgewählt
CN- INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- OBJECT_TERMINATED-2	Objekt befindet sich nicht im Zustand "terminated"
CN- SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.3.4 APDU-Kommandos

ID: CM-ACTIVATE_FILE_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

2.3.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6986	Das Testsystem antwortet mit '69 86'.

2.3.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_FILE-2	Das entsprechende File ist nicht auslesbar.

2.4 Testfall: ACTIVATE FILE (TC_ACTIVATE_FILE_FF_3)

2.4.1 Informationen

ID	TC_ACTIVATE_FILE_FF_3

Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE FILE nicht erfolgreich durchgeführt werden kann, wenn sich das Objekt im Zustand "terminated" befindet. Dazu wird eine Kommandonachricht für ACTIVATE FILE zur Aktivierung eines DFs/EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.4.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.4

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.4.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_TERMINATED-1	Objekt befindet sich im Zustand "terminated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_CURRENT_FILE-2	Das File ist ausgewählt
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.4.4 APDU-Kommandos

ID: CM-ACTIVATE_FILE_FF_3

CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

2.4.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.4.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_FILE-2	Das entsprechende File ist nicht auslesbar.

2.5 Testfall: ACTIVATE FILE (TC_ACTIVATE_FILE_FF_4_1)

2.5.1 Informationen

ID	TC_ACTIVATE_FILE_FF_4_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE FILE nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Nicht erfüllt bedeutet in diesem Testfall, dass eine notwendige Authentifizierung fehlt. Dazu wird eine Kommandonachricht für ACTIVATE FILE zur Aktivierung eines DFs/EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.5.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.4

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.5.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt (Authentifizierung nicht durchgeführt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_CURRENT_FILE-2	Das File ist ausgewählt
CN-OBJECT_TERMINATED-2	Objekt befindet sich nicht im Zustand "terminated"

2.5.4 APDU-Kommandos

ID: CM-ACTIVATE_FILE_FF_4_1						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

2.5.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.5.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_FILE-2	Das entsprechende File ist nicht auslesbar.

2.6 Testfall: ACTIVATE FILE (TC_ACTIVATE_FILE_FF_4_2)

2.6.1 Informationen

ID	TC_ACTIVATE_FILE_FF_4_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE FILE nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Nicht erfüllt bedeutet in diesem Testfall, dass der notwendige PACE-Kanal nicht aufgebaut ist. Dazu wird eine Kommandonachricht für ACTIVATE FILE zur Aktivierung eines DFs/EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.6.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.4

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.6.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt (PACE-Kanal nicht aufgebaut)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-CURRENT_FILE-2	Das File ist ausgewählt

CN- OBJECT_TERMINA TED-2	Objekt befindet sich nicht im Zustand "terminated"

2.6.4 APDU-Kommandos

ID: CM-ACTIVATE_FILE_FF_4_2						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

2.6.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.6.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_FILE-2	Das entsprechende File ist nicht auslesbar.

2.7 Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_GF_1_1)

2.7.1 Informationen

ID	TC_ACTIVATE_KEY_GF_1_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Key-Objekt ist in diesem Fall ein Public-Key-Objekt für AT. Dazu wird eine Kommandonachricht für ACTIVATE KEY zur Aktivierung eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.7.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.7.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.7.4 APDU-Kommandos

ID: CM-ACTIVATE_KEY_GF_1_1						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	08	a4 06 [83 04 [00 00 00 13]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.7.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.7.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_KEY-1	Das entsprechende Key-Objekt ist auslesbar.

2.8 Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_GF_1_2)

2.8.1 Informationen

ID	TC_ACTIVATE_KEY_GF_1_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Key-Objekt ist in diesem Fall ein Public-Key-Objekt für DST. Dazu wird eine Kommandonachricht für ACTIVATE KEY zur Aktivierung eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.8.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.8.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRE	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CTNESS	
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.8.4 APDU-Kommandos

ID: CM-ACTIVATE_KEY_GF_1_2						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	08	b6 06 [83 04 [00 00 00 11]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.8.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.8.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_KEY-1	Das entsprechende Key-Objekt ist auslesbar.

2.9 Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_GF_1_3)

2.9.1 Informationen

ID	TC_ACTIVATE_KEY_GF_1_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Key-Objekt ist in diesem Fall ein Public-Key-Objekt für AT. Dazu wird eine Kommandonachricht für ACTIVATE KEY zur Aktivierung eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.9.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.9.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

SECURITY_STATU S_NOT_SATISFIED- 2	

2.9.4 APDU-Kommandos

ID: CM-ACTIVATE_KEY_GF_1_3						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	05	a4 03 [84 01 [03]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.9.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.9.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_KEY-1	Das entsprechende Key-Objekt ist auslesbar.

2.10 Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_GF_1_4)

2.10.1 Informationen

ID	TC_ACTIVATE_KEY_GF_1_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Key-Objekt ist in diesem Fall ein Public-Key-Objekt für DST. Dazu wird eine Kommandonachricht für ACTIVATE KEY zur Aktivierung eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die

	inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.10.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.10.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.10.4 APDU-Kommandos

ID: CM-ACTIVATE_KEY_GF_1_4						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	05	b6 03 [84 01 [31]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.10.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.10.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_KEY-1	Das entsprechende Key-Objekt ist auslesbar.

2.11 Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_1)

2.11.1 Informationen

ID	TC_ACTIVATE_KEY_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für ACTIVATE KEY zur Aktivierung eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.11.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.11.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.11.4 APDU-Kommandos

ID: CM-ACTIVATE_KEY_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	08	a4 06 [83 04 [00 00 00 13]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.11.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.11.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_KEY-2	Das entsprechende Key-Objekt ist nicht auslesbar.

2.12 Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_2_1)

2.12.1 Informationen

ID	TC_ACTIVATE_KEY_FF_2_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt für AT doppelt vorhanden ist. Dazu wird eine Kommandonachricht für ACTIVATE KEY zur Aktivierung eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.12.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.12.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Doppelt vorhandenes Datenobjekt für AT)

CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.12.4 APDU-Kommandos

ID: CM-ACTIVATE_KEY_FF_2_1						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	08	a4 06 [83 04 [00 00 00 13]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.12.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.12.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_KEY-2	Das entsprechende Key-Objekt ist nicht auslesbar.

2.13 Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_2_2)

2.13.1 Informationen

ID	TC_ACTIVATE_KEY_FF_2_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt für DST doppelt vorhanden ist. Dazu wird eine Kommandonachricht für ACTIVATE KEY zur Aktivierung eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.13.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.13.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Doppelt vorhandenes Datenobjekt für DST)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

SECURITY_STATU S_NOT_SATISFIED- 2	

2.13.4 APDU-Kommandos

ID: CM-ACTIVATE_KEY_FF_2_2						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	08	b6 06 [83 04 [00 00 00 11]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.13.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.13.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_KEY-2	Das entsprechende Key-Objekt ist nicht auslesbar.

2.14 Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_2_3)

2.14.1 Informationen

ID	TC_ACTIVATE_KEY_FF_2_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt für AT ein falsches Tag besitzt. Dazu wird eine Kommandonachricht für ACTIVATE KEY zur Aktivierung eines Key-

	Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.14.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.14.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für AT)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.14.4 APDU-Kommandos

ID: CM-ACTIVATE_KEY_FF_2_3						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	08	a4 06 [83 04 [00 00 00 13]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.14.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.14.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_KEY-2	Das entsprechende Key-Objekt ist nicht auslesbar.

2.15 Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_2_4)

2.15.1 Informationen

ID	TC_ACTIVATE_KEY_FF_2_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt für DST ein falsches Tag besitzt. Dazu wird eine Kommandonachricht für ACTIVATE KEY zur Aktivierung eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.15.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.15.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für DST)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.15.4 APDU-Kommandos

ID: CM-ACTIVATE_KEY_FF_2_4						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	08	b6 06 [83 04 [00 00 00 11]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.15.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.15.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_KEY-2	Das entsprechende Key-Objekt ist nicht auslesbar.

2.16 Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_2_5)

2.16.1 Informationen

ID	TC_ACTIVATE_KEY_FF_2_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt für das Key-Pair-Objekt ein falsches Tag besitzt. Dazu wird eine Kommandonachricht für ACTIVATE KEY zur Aktivierung eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.16.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.16.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für das Key-Pair-Objekt)

CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.16.4 APDU-Kommandos

ID: CM-ACTIVATE_KEY_FF_2_5						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	05	a4 03 [84 01 [03]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.16.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.16.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_KEY-2	Das entsprechende Key-Objekt ist nicht auslesbar.

2.17 Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_2_6)

2.17.1 Informationen

ID	TC_ACTIVATE_KEY_FF_2_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt für das Public-Key-Objekt ein falsches Tag besitzt. Dazu wird eine Kommandonachricht für ACTIVATE KEY zur Aktivierung eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.17.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.17.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für das Public-Key-Objekt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

SECURITY_STATU S_NOT_SATISFIED- 2	

2.17.4 APDU-Kommandos

ID: CM-ACTIVATE_KEY_FF_2_6						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	08	a4 06 [83 04 [00 00 00 13]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.17.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.17.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_KEY-2	Das entsprechende Key-Objekt ist nicht auslesbar.

2.18 Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_2_7)

2.18.1 Informationen

ID	TC_ACTIVATE_KEY_FF_2_7
Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt einen zu langen Key-Namen für das Key-Pair-Objekt besitzt. Dazu wird eine Kommandonachricht für ACTIVATE KEY zur

	Aktivierung eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.18.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.18.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit zu langen Key-Namen für null)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.18.4 APDU-Kommandos

ID: CM-ACTIVATE_KEY_FF_2_7							
CLA	INS	P1	P2	Lc	Data		Le

00	44	21	00	05	a4 03 [84 01 [03]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.18.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.18.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_KEY-2	Das entsprechende Key-Objekt ist nicht auslesbar.

2.19 Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_2_8)

2.19.1 Informationen

ID	TC_ACTIVATE_KEY_FF_2_8
Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt einen zu langen Key-Namen für das Public-Key-Objekt besitzt. Dazu wird eine Kommandonachricht für ACTIVATE KEY zur Aktivierung eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.19.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.19.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit zu langen Key-Namen für null)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.19.4 APDU-Kommandos

ID: CM-ACTIVATE_KEY_FF_2_8						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	08	a4 06 [83 04 [00 00 00 13]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.19.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.19.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_KEY-2	Das entsprechende Key-Objekt ist nicht auslesbar.

2.20 Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_3_1)

2.20.1 Informationen

ID	TC_ACTIVATE_KEY_FF_3_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn das Key-Pair-Objekt für AT nicht gefunden wird. Dazu wird eine Kommandonachricht für ACTIVATE KEY zur Aktivierung eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.20.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.20.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-	Key-Pair-Objekt für AT kann nicht gefunden werden

1	
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.20.4 APDU-Kommandos

ID: CM-ACTIVATE_KEY_FF_3_1						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	05	a4 03 [84 01 [03]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.20.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.20.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_KEY-2	Das entsprechende Key-Objekt ist nicht auslesbar.

2.21 Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_3_2)

2.21.1 Informationen

ID	TC_ACTIVATE_KEY_FF_3_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn das Key-Pair-Objekt für DST nicht gefunden wird. Dazu wird eine Kommandonachricht für ACTIVATE KEY zur Aktivierung eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.21.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.21.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	Key-Pair-Objekt für DST kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN-SECURITY_STATUS	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

S_NOT_SATISFIED-2	

2.21.4 APDU-Kommandos

ID: CM-ACTIVATE_KEY_FF_3_2						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	05	b6 03 [84 01 [31]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.21.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.21.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_KEY-2	Das entsprechende Key-Objekt ist nicht auslesbar.

2.22 Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_3_3)

2.22.1 Informationen

ID	TC_ACTIVATE_KEY_FF_3_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn das Public-Key-Objekt für AT nicht gefunden wird. Dazu wird eine Kommandonachricht für ACTIVATE KEY zur Aktivierung eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird

	im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.22.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.22.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	Public-Key-Objekt für AT kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.22.4 APDU-Kommandos

ID: CM-ACTIVATE_KEY_FF_3_3						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	08	a4 06 [83 04 [00 00 00 13]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.22.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.22.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_KEY-2	Das entsprechende Key-Objekt ist nicht auslesbar.

2.23 Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_3_4)

2.23.1 Informationen

ID	TC_ACTIVATE_KEY_FF_3_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn das Public-Key-Objekt für DST nicht gefunden wird. Dazu wird eine Kommandonachricht für ACTIVATE KEY zur Aktivierung eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.23.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.23.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	Public-Key-Objekt für DST kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.23.4 APDU-Kommandos

ID: CM-ACTIVATE_KEY_FF_3_4						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	08	b6 06 [83 04 [00 00 00 11]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.23.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.23.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_KEY-2	Das entsprechende Key-Objekt ist nicht auslesbar.

2.24 Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_4_1)

2.24.1 Informationen

ID	TC_ACTIVATE_KEY_FF_4_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Nicht erfüllt bedeutet in diesem Testfall, dass eine notwendige Authentifizierung fehlt. Dazu wird eine Kommandonachricht für ACTIVATE KEY zur Aktivierung eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.24.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.24.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt (Authentifizierung nicht durchgeführt)

CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden

2.24.4 APDU-Kommandos

ID: CM-ACTIVATE_KEY_FF_4_1						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	08	a4 06 [83 04 [00 00 00 13]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.24.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.24.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_KEY-2	Das entsprechende Key-Objekt ist nicht auslesbar.

2.25 Testfall: ACTIVATE KEY (TC_ACTIVATE_KEY_FF_4_2)

2.25.1 Informationen

ID	TC_ACTIVATE_KEY_FF_4_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando ACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Nicht erfüllt bedeutet in diesem Testfall, dass der notwendige PACE-Kanal nicht aufgebaut ist. Dazu wird eine Kommandonachricht für ACTIVATE KEY zur Aktivierung eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.25.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_07

2.25.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt (PACE-Kanal nicht aufgebaut)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)

CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden

2.25.4 APDU-Kommandos

ID: CM-ACTIVATE_KEY_FF_4_2						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	08	a4 06 [83 04 [00 00 00 13]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.25.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.25.6 Verifikationen

ID	Beschreibung
VF-ACTIVATE_KEY-2	Das entsprechende Key-Objekt ist nicht auslesbar.

2.26 Testfall: APPEND RECORD ohne SFI (TC_APPEND_RECORD_WITHOUT_SFI_GF_1)

2.26.1 Informationen

ID	TC_APPEND_RECORD_WITHOUT_SFI_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando APPEND RECORD ohne SFI erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für

	APPEND RECORD ohne SFI zum Anlegen eines weiteren Record in einem record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.26.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.5

2.26.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-FULL_EF-2	Speicherplatz des EF reicht aus
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NOT_CURRENT_EF-2	Das EF ist ausgewählt
CN-OUT_OF_MEMORY-2	Speicherplatz des EF reicht aus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist strukturiert
CN-WRONG_RECORD_	Parameter "neue Daten" passt zur zulässigen Record-Länge

LENGTH-2	

2.26.4 APDU-Kommandos

ID: CM-APPEND_RECORD_WITHOUT_SFI_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

2.26.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.26.6 Verifikationen

ID	Beschreibung
VF-APPEND_RECORD_WITHOUT_SFI-1	Das entsprechende EF enthält den hinzugefügten Record.

2.27 Testfall: APPEND RECORD ohne SFI (TC_APPEND_RECORD_WITHOUT_SFI_FF_1)

2.27.1 Informationen

ID	TC_APPEND_RECORD_WITHOUT_SFI_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando APPEND RECORD ohne SFI nicht erfolgreich durchgeführt werden kann, wenn der Speicherplatz des EF nicht ausreicht. Dazu wird eine Kommandonachricht für APPEND RECORD ohne SFI zum Anlegen eines weiteren Record in einem record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.

Klassifizierung	Fehlerfall-Test

2.27.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.5

2.27.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-FULL_EF-1	Speicherplatz des EF reicht nicht aus
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_CURRENT_EF-2	Das EF ist ausgewählt
CN-OUT_OF_MEMORY-2	Speicherplatz des EF reicht aus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist strukturiert
CN-WRONG_RECORD_LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge

2.27.4 APDU-Kommandos

ID: CM-APPEND_RECORD_WITHOUT_SFI_FF_1

CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

2.27.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A84	Das Testsystem antwortet mit '6a 84'.

2.27.6 Verifikationen

ID	Beschreibung
VF-APPEND_RECORD_WITHOUT_SFI-2	Das entsprechende EF enthält den hinzugefügten Record nicht.

2.28 Testfall: APPEND RECORD ohne SFI (TC_APPEND_RECORD_WITHOUT_SFI_FF_2)

2.28.1 Informationen

ID	TC_APPEND_RECORD_WITHOUT_SFI_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando APPEND RECORD ohne SFI nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für APPEND RECORD ohne SFI zum Anlegen eines weiteren Record in einem record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.28.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.5

2.28.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-FULL_EF-2	Speicherplatz des EF reicht aus
CN-NO_CURRENT_EF-2	Das EF ist ausgewählt
CN-OUT_OF_MEMORY-2	Speicherplatz des EF reicht aus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist strukturiert
CN-WRONG_RECORD_LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge

2.28.4 APDU-Kommandos

ID: CM-APPEND_RECORD_WITHOUT_SFI_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

2.28.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.28.6 Verifikationen

ID	Beschreibung
VF-APPEND_RECORD_WITHOUT_SFI-2	Das entsprechende EF enthält den hinzugefügten Record nicht.

2.29 Testfall: APPEND RECORD ohne SFI (TC_APPEND_RECORD_WITHOUT_SFI_FF_3)

2.29.1 Informationen

ID	TC_APPEND_RECORD_WITHOUT_SFI_FF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando APPEND RECORD ohne SFI nicht erfolgreich durchgeführt werden kann, wenn kein EF selektiert ist. Dazu wird eine Kommandonachricht für APPEND RECORD ohne SFI zum Anlegen eines weiteren Record in einem record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.29.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.5

2.29.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRE	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CTNESS	
CN- NO_CURRENT_EF- 1	Das EF ist nicht ausgewählt
CN-FULL_EF-2	Speicherplatz des EF reicht aus
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- OUT_OF_MEMORY -2	Speicherplatz des EF reicht aus
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN- WRONG_FILE_TYP E-2	Ausgewähltes EF ist strukturiert
CN- WRONG_RECORD_ LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge

2.29.4 APDU-Kommandos

ID: CM-APPEND_RECORD_WITHOUT_SFI_FF_3						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

2.29.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6986	Das Testsystem antwortet mit '69 86'.

2.29.6 Verifikationen

ID	Beschreibung
VF-APPEND_RECORD_WITHOUT_SFI-2	Das entsprechende EF enthält den hinzugefügten Record nicht.

2.30 Testfall: APPEND RECORD ohne SFI (TC_APPEND_RECORD_WITHOUT_SFI_FF_4)

2.30.1 Informationen

ID	TC_APPEND_RECORD_WITHOUT_SFI_FF_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando APPEND RECORD ohne SFI nicht erfolgreich durchgeführt werden kann, wenn der restliche Speicherplatz des EF nicht ausreicht, d. h. wenn die maximale Anzahl an Records im adressierten EF erreicht ist und dieses kein Anhängen weiterer Records erlaubt. Dazu wird eine Kommandonachricht für APPEND RECORD ohne SFI zum Anlegen eines weiteren Record in einem record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.30.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.5

2.30.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OUT_OF_MEMORY-1	Speicherplatz des EF reicht nicht aus

CN-FULL_EF-2	Speicherplatz des EF reicht aus
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_CURRENT_EF-2	Das EF ist ausgewählt
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist strukturiert
CN-WRONG_RECORD_LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge

2.30.4 APDU-Kommandos

ID: CM-APPEND_RECORD_WITHOUT_SFI_FF_4						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

2.30.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A84	Das Testsystem antwortet mit '6a 84'.

2.30.6 Verifikationen

ID	Beschreibung
VF-APPEND_RECORD_WITHOUT_SFI-2	Das entsprechende EF enthält den hinzugefügten

	Record nicht.

2.31 Testfall: APPEND RECORD ohne SFI (TC_APPEND_RECORD_WITHOUT_SFI_FF_5)

2.31.1 Informationen

ID	TC_APPEND_RECORD_WITHOUT_SFI_FF_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando APPEND RECORD ohne SFI nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Dazu wird eine Kommandonachricht für APPEND RECORD ohne SFI zum Anlegen eines weiteren Record in einem record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.31.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.5

2.31.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-FULL_EF-2	Speicherplatz des EF reicht aus
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN- NO_CURRENT_EF- 2	Das EF ist ausgewählt
CN- OUT_OF_MEMORY -2	Speicherplatz des EF reicht aus
CN- WRONG_FILE_TYP E-2	Ausgewähltes EF ist strukturiert
CN- WRONG_RECORD_ LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge

2.31.4 APDU-Kommandos

ID: CM-APPEND_RECORD_WITHOUT_SFI_FF_5						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

2.31.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.31.6 Verifikationen

ID	Beschreibung
VF-APPEND_RECORD_WITHOUT_SFI-2	Das entsprechende EF enthält den hinzugefügten Record nicht.

2.32 Testfall: APPEND RECORD ohne SFI (TC_APPEND_RECORD_WITHOUT_SFI_FF_6)

2.32.1 Informationen

ID	TC_APPEND_RECORD_WITHOUT_SFI_FF_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando APPEND RECORD ohne SFI nicht erfolgreich durchgeführt werden kann, wenn das ausgewählte EF keine Record-basierte Struktur aufweist. Dazu wird eine Kommandonachricht für APPEND RECORD ohne SFI zum Anlegen eines weiteren Record in einem record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.32.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.5

2.32.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-WRONG_FILE_TYPE-1	Ausgewähltes EF ist nicht strukturiert
CN-FULL_EF-2	Speicherplatz des EF reicht aus
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NOT_CURRENT_EF-2	Das EF ist ausgewählt

CN- OUT_OF_MEMORY-2	Speicherplatz des EF reicht aus
CN- SECURITY_STATU S_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN- WRONG_RECORD_ LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge

2.32.4 APDU-Kommandos

ID: CM-APPEND_RECORD_WITHOUT_SFI_FF_6						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

2.32.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6981	Das Testsystem antwortet mit '69 81'.

2.32.6 Verifikationen

ID	Beschreibung
VF-APPEND_RECORD_WITHOUT_SFI-2	Das entsprechende EF enthält den hinzugefügten Record nicht.

2.33 Testfall: APPEND RECORD ohne SFI (TC_APPEND_RECORD_WITHOUT_SFI_FF_7)

2.33.1 Informationen

ID	TC_APPEND_RECORD_WITHOUT_SFI_FF_7
Beschreibung	Dieser Test verifiziert, dass ein Kommando APPEND RECORD ohne SFI nicht erfolgreich durchgeführt werden kann, wenn die Länge der an das File anzuhängenden Daten nicht zulässig ist. Dazu wird eine Kommandonachricht für APPEND RECORD ohne SFI zum Anlegen eines weiteren Record in einem record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.33.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.5

2.33.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-WRONG_RECORD_LENGTH-1	Parameter "neue Daten" passt nicht zur zulässigen Record-Länge
CN-FULL_EF-2	Speicherplatz des EF reicht aus
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NOT_CURRENT_EF-2	Das EF ist ausgewählt

CN- OUT_OF_MEMORY -2	Speicherplatz des EF reicht aus
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN- WRONG_FILE_TYP E-2	Ausgewähltes EF ist strukturiert

2.33.4 APDU-Kommandos

ID: CM-APPEND_RECORD_WITHOUT_SFI_FF_7						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

2.33.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A87	Das Testsystem antwortet mit '6a 87'.

2.33.6 Verifikationen

ID	Beschreibung
VF-APPEND_RECORD_WITHOUT_SFI-2	Das entsprechende EF enthält den hinzugefügten Record nicht.

2.34 Testfall: APPEND RECORD mit SFI (TC_APPEND_RECORD_WITH_SFI_GF_1)

2.34.1 Informationen

ID	TC_APPEND_RECORD_WITH_SFI_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando APPEND RECORD mit SFI erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für APPEND RECORD mit SFI zum Anlegen eines weiteren Record in einem record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.34.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.5

2.34.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-	Ausgewähltes EF ist strukturiert

WRONG_FILE_TYPE-2	
CN-FULL_EF-2	Speicherplatz des EF reicht aus
CN-OUT_OF_MEMORY-2	Speicherplatz des EF reicht aus
CN-WRONG_RECORD_LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge

2.34.4 APDU-Kommandos

ID: CM-APPEND_RECORD_WITH_SFI_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	XX	LL	XX...XX	--

'P2' enthält den SFI (mit $SFI < 3$).

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

2.34.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.34.6 Verifikationen

ID	Beschreibung
VF-APPEND_RECORD_WITH_SFI-1	Das entsprechende EF enthält den hinzugefügten Record.

2.35 Testfall: APPEND RECORD mit SFI (TC_APPEND_RECORD_WITH_SFI_FF_1)

2.35.1 Informationen

ID	TC_APPEND_RECORD_WITH_SFI_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando APPEND RECORD mit SFI nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für APPEND RECORD mit SFI zum Anlegen eines weiteren Record in einem record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.35.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.5

2.35.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist strukturiert
CN-FULL_EF-2	Speicherplatz des EF reicht aus
CN-OUT_OF_MEMORY-2	Speicherplatz des EF reicht aus
CN-WRONG_RECORD_LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge

2.35.4 APDU-Kommandos

ID: CM-APPEND_RECORD_WITH_SFI_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	XX	LL	XX...XX	--

'P2' enthält den SFI (mit $SFI < 3$).

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

2.35.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.35.6 Verifikationen

ID	Beschreibung
VF-APPEND_RECORD_WITH_SFI-2	Das entsprechende EF enthält den hinzugefügten Record nicht.

2.36 Testfall: APPEND RECORD mit SFI (TC_APPEND_RECORD_WITH_SFI_FF_2)

2.36.1 Informationen

ID	TC_APPEND_RECORD_WITH_SFI_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando APPEND RECORD mit SFI nicht erfolgreich durchgeführt werden kann, wenn das per SFI adressierte File nicht gefunden werden kann. Dazu wird eine Kommandonachricht für APPEND RECORD mit SFI zum Anlegen eines weiteren Record in einem record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.36.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.5

2.36.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-FILE_NOT_FOUND-1	Das per SFI adressierte File kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-	Ausgewähltes EF ist strukturiert

WRONG_FILE_TYPE-2	
CN-FULL_EF-2	Speicherplatz des EF reicht aus
CN-OUT_OF_MEMORY-2	Speicherplatz des EF reicht aus
CN-WRONG_RECORD_LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge

2.36.4 APDU-Kommandos

ID: CM-APPEND_RECORD_WITH_SFI_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	XX	LL	XX...XX	--

'P2' enthält den SFI (mit $SFI < 3$).

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

2.36.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A82	Das Testsystem antwortet mit '6a 82'.

2.36.6 Verifikationen

ID	Beschreibung
VF-APPEND_RECORD_WITH_SFI-2	Das entsprechende EF enthält den hinzugefügten Record nicht.

2.37 Testfall: APPEND RECORD mit SFI (TC_APPEND_RECORD_WITH_SFI_FF_3)

2.37.1 Informationen

ID	TC_APPEND_RECORD_WITH_SFI_FF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando APPEND RECORD mit SFI nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Dazu wird eine Kommandonachricht für APPEND RECORD mit SFI zum Anlegen eines weiteren Record in einem record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.37.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.5

2.37.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden

CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist strukturiert
CN-FULL_EF-2	Speicherplatz des EF reicht aus
CN-OUT_OF_MEMORY-2	Speicherplatz des EF reicht aus
CN-WRONG_RECORD_LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge

2.37.4 APDU-Kommandos

ID: CM-APPEND_RECORD_WITH_SFI_FF_3						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	XX	LL	XX...XX	--

'P2' enthält den SFI (mit $SFI < 3$).

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

2.37.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.37.6 Verifikationen

ID	Beschreibung
VF-APPEND_RECORD_WITH_SFI-2	Das entsprechende EF enthält den hinzugefügten Record nicht.

2.38 Testfall: APPEND RECORD mit SFI (TC_APPEND_RECORD_WITH_SFI_FF_4)

2.38.1 Informationen

ID	TC_APPEND_RECORD_WITH_SFI_FF_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando APPEND RECORD mit SFI nicht erfolgreich durchgeführt werden kann, wenn das ausgewählte EF keine Record-basierte Struktur aufweist. Dazu wird eine Kommandonachricht für APPEND RECORD mit SFI zum Anlegen eines weiteren Record in einem record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.38.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.5

2.38.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-WRONG_FILE_TYPE-1	Ausgewähltes EF ist nicht strukturiert
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden
CN-	Zugriffsregel ist erfüllt

SECURITY_STATU S_NOT_SATISFIED- 2	
CN-FULL_EF-2	Speicherplatz des EF reicht aus
CN- OUT_OF_MEMORY -2	Speicherplatz des EF reicht aus
CN- WRONG_RECORD_ LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge

2.38.4 APDU-Kommandos

ID: CM-APPEND_RECORD_WITH_SFI_FF_4						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	XX	LL	XX...XX	--

'P2' enthält den SFI (mit $SFI < 3$).

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

2.38.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6981	Das Testsystem antwortet mit '69 81'.

2.38.6 Verifikationen

ID	Beschreibung
VF-APPEND_RECORD_WITH_SFI-2	Das entsprechende EF enthält den hinzugefügten Record nicht.

2.39 Testfall: APPEND RECORD mit SFI (TC_APPEND_RECORD_WITH_SFI_FF_5)

2.39.1 Informationen

ID	TC_APPEND_RECORD_WITH_SFI_FF_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando APPEND RECORD mit SFI nicht erfolgreich durchgeführt werden kann, wenn der Speicherplatz des EF nicht ausreicht. Dazu wird eine Kommandonachricht für APPEND RECORD mit SFI zum Anlegen eines weiteren Record in einem record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.39.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.5

2.39.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-FULL_EF-1	Speicherplatz des EF reicht nicht aus
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist strukturiert
CN-OUT_OF_MEMORY-2	Speicherplatz des EF reicht aus
CN-WRONG_RECORD_LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge

2.39.4 APDU-Kommandos

ID: CM-APPEND_RECORD_WITH_SFI_FF_5						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	XX	LL	XX...XX	--

'P2' enthält den SFI (mit $SFI < 3$).

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

2.39.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A84	Das Testsystem antwortet mit '6a 84'.

2.39.6 Verifikationen

ID	Beschreibung
VF-APPEND_RECORD_WITH_SFI-2	Das entsprechende EF enthält den hinzugefügten Record nicht.

2.40 Testfall: APPEND RECORD mit SFI (TC_APPEND_RECORD_WITH_SFI_FF_6)

2.40.1 Informationen

ID	TC_APPEND_RECORD_WITH_SFI_FF_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando APPEND RECORD mit SFI nicht erfolgreich durchgeführt werden kann, wenn der restliche Speicherplatz des EF nicht ausreicht, d. h. wenn die maximale Anzahl an Records im adressierten EF erreicht ist und dieses kein Anhängen weiterer Records erlaubt. Dazu wird eine Kommandonachricht für APPEND RECORD mit SFI zum Anlegen eines weiteren Record in einem record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.40.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.5

2.40.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OUT_OF_MEMORY-1	Speicherplatz des EF reicht nicht aus
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden

CN-SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN-WRONG_FILE_TYP E-2	Ausgewähltes EF ist strukturiert
CN-FULL_EF-2	Speicherplatz des EF reicht aus
CN-WRONG_RECORD_ LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge

2.40.4 APDU-Kommandos

ID: CM-APPEND_RECORD_WITH_SFI_FF_6						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	XX	LL	XX...XX	--

'P2' enthält den SFI (mit $SFI < 3$).

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

2.40.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A84	Das Testsystem antwortet mit '6a 84'.

2.40.6 Verifikationen

ID	Beschreibung
VF-APPEND_RECORD_WITH_SFI-2	Das entsprechende EF enthält den hinzugefügten Record nicht.

2.41 Testfall: APPEND RECORD mit SFI (TC_APPEND_RECORD_WITH_SFI_FF_7)

2.41.1 Informationen

ID	TC_APPEND_RECORD_WITH_SFI_FF_7
Beschreibung	Dieser Test verifiziert, dass ein Kommando APPEND RECORD mit SFI nicht erfolgreich durchgeführt werden kann, wenn die Länge der an das File anzuhängenden Daten nicht zulässig ist. Dazu wird eine Kommandonachricht für APPEND RECORD mit SFI zum Anlegen eines weiteren Record in einem record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.41.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.5

2.41.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-WRONG_RECORD_LENGTH-1	Parameter "neue Daten" passt nicht zur zulässigen Record-Länge
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden
CN-	Zugriffsregel ist erfüllt

SECURITY_STATU S_NOT_SATISFIED- 2	
CN- WRONG_FILE_TYP E-2	Ausgewähltes EF ist strukturiert
CN-FULL_EF-2	Speicherplatz des EF reicht aus
CN- OUT_OF_MEMORY -2	Speicherplatz des EF reicht aus

2.41.4 APDU-Kommandos

ID: CM-APPEND_RECORD_WITH_SFI_FF_7						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	XX	LL	XX...XX	--

'P2' enthält den SFI (mit $SFI < 3$).

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

2.41.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A87	Das Testsystem antwortet mit '6a 87'.

2.41.6 Verifikationen

ID	Beschreibung
VF-APPEND_RECORD_WITH_SFI-2	Das entsprechende EF enthält den hinzugefügten Record nicht.

2.42 Testfall: CHANGE REFERENCE DATA zum Wechseln der PIN (TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_GF_1_1)

2.42.1 Informationen

ID	TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_GF_1_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando CHANGE REFERENCE DATA zum Wechseln der PIN erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Es erfolgt ein Wechsel auf die ursprüngliche PIN. Dazu wird eine Kommandonachricht für CHANGE REFERENCE DATA zum Wechseln der PIN zum Wechseln einer PIN an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.42.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.8.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_02

2.42.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PASSWORD_NOT_FOUND-2	Das PIN-Objekt kann gefunden werden

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN- LONG_PASSWORD -2	Neue PIN ist nicht zu lang
CN- SHORT_PASSWOR D-2	Neue PIN ist nicht zu kurz
CN- OBJECT_INITIALIZ ATION-2	PIN-Objekt befindet sich nicht im Zustand "initialisation"

2.42.4 APDU-Kommandos

ID: CM-CHANGE_REFERENCE_DATA_CHANGE_PIN_GF_1_1						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

2.42.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.42.6 Verifikationen

ID	Beschreibung
VF- CHANGE_REFERENCE_DATA_CHANGE_P IN-1	Die PIN ist gegenüber dem Wert vor Ausführung des Testfalls verändert.

2.43 Testfall: CHANGE REFERENCE DATA zum Wechseln der PIN (TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_GF_1_2)

2.43.1 Informationen

ID	TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_GF_1_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando CHANGE REFERENCE DATA zum Wechseln der PIN erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Es erfolgt ein Wechsel auf eine längere PIN. Dazu wird eine Kommandonachricht für CHANGE REFERENCE DATA zum Wechseln der PIN zum Wechseln einer PIN an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.43.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.8.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_02

2.43.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PASSWORD_NOT_FOUND-2	Das PIN-Objekt kann gefunden werden

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN- LONG_PASSWORD -2	Neue PIN ist nicht zu lang
CN- SHORT_PASSWOR D-2	Neue PIN ist nicht zu kurz
CN- OBJECT_INITIALIZ ATION-2	PIN-Objekt befindet sich nicht im Zustand "initialisation"

2.43.4 APDU-Kommandos

ID: CM-CHANGE_REFERENCE_DATA_CHANGE_PIN_GF_1_2						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

2.43.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.43.6 Verifikationen

ID	Beschreibung
VF- CHANGE_REFERENCE_DATA_CHANGE_P IN-1	Die PIN ist gegenüber dem Wert vor Ausführung des Testfalls verändert.

2.44 Testfall: CHANGE REFERENCE DATA zum Wechseln der PIN (TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_GF_1_3)

2.44.1 Informationen

ID	TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_GF_1_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando CHANGE REFERENCE DATA zum Wechseln der PIN erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Es erfolgt ein Wechsel auf eine kürzere PIN. Dazu wird eine Kommandonachricht für CHANGE REFERENCE DATA zum Wechseln der PIN zum Wechseln einer PIN an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.44.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.8.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_02

2.44.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PASSWORD_NOT_FOUND-2	Das PIN-Objekt kann gefunden werden

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN- LONG_PASSWORD -2	Neue PIN ist nicht zu lang
CN- SHORT_PASSWOR D-2	Neue PIN ist nicht zu kurz
CN- OBJECT_INITIALIZ ATION-2	PIN-Objekt befindet sich nicht im Zustand "initialisation"

2.44.4 APDU-Kommandos

ID: CM-CHANGE_REFERENCE_DATA_CHANGE_PIN_GF_1_3						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

2.44.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.44.6 Verifikationen

ID	Beschreibung
VF- CHANGE_REFERENCE_DATA_CHANGE_P IN-1	Die PIN ist gegenüber dem Wert vor Ausführung des Testfalls verändert.

2.45 Testfall: CHANGE REFERENCE DATA zum Wechseln der PIN (TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_GF_2)

2.45.1 Informationen

ID	TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_GF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando CHANGE REFERENCE DATA zum Wechseln der PIN erfolgreich abgelehnt wird, wenn die alte PIN falsch ist. Dazu wird eine Kommandonachricht für CHANGE REFERENCE DATA zum Wechseln der PIN zum Wechseln einer PIN an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.45.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.8.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_02

2.45.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PASSWORD_NOT_FOUND-2	Das PIN-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)

2	
CN-LONG_PASSWORD-2	Neue PIN ist nicht zu lang
CN-SHORT_PASSWORD-2	Neue PIN ist nicht zu kurz
CN-OBJECT_INITIALIZATION-2	PIN-Objekt befindet sich nicht im Zustand "initialisation"

2.45.4 APDU-Kommandos

ID: CM-CHANGE_REFERENCE_DATA_CHANGE_PIN_GF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

2.45.5 Erwartete Ergebnisse

ID	Beschreibung
RS-D5D4	63 cX

2.45.6 Verifikationen

ID	Beschreibung
VF-CHANGE_REFERENCE_DATA_CHANGE_PIN-1	Die PIN ist gegenüber dem Wert vor Ausführung des Testfalls verändert.

2.46 Testfall: CHANGE REFERENCE DATA zum Wechseln der PIN (TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_1)

2.46.1 Informationen

ID	TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando CHANGE REFERENCE DATA zum Wechseln der PIN nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für CHANGE REFERENCE DATA zum Wechseln der PIN zum Wechseln einer PIN an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.46.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.8.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_02

2.46.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-PASSWORD_NOT_FOUND-2	Das PIN-Objekt kann gefunden werden
CN-SECURITY_STATUS	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)

S_NOT_SATISFIED-2	
CN-LONG_PASSWORD-2	Neue PIN ist nicht zu lang
CN-SHORT_PASSWORD-2	Neue PIN ist nicht zu kurz
CN-OBJECT_INITIALIZATION-2	PIN-Objekt befindet sich nicht im Zustand "initialisation"

2.46.4 APDU-Kommandos

ID: CM-CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

2.46.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.46.6 Verifikationen

ID	Beschreibung
VF-CHANGE_REFERENCE_DATA_CHANGE_PIN-2	Die PIN ist gegenüber dem Wert vor Ausführung des Testfalls nicht verändert.

2.47 Testfall: CHANGE REFERENCE DATA zum Wechseln der PIN (TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_2)

2.47.1 Informationen

ID	TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando CHANGE REFERENCE DATA zum Wechseln der PIN nicht erfolgreich durchgeführt werden kann, wenn das mittels P2-Parameter adressierte PIN-Objekt nicht gefunden wird. Dazu wird eine Kommandonachricht für CHANGE REFERENCE DATA zum Wechseln der PIN zum Wechseln einer PIN an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.47.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.8.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_02

2.47.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-PASSWORD_NOT_FOUND-1	Das PIN-Objekt kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUS	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)

S_NOT_SATISFIED-2	
CN-LONG_PASSWORD-2	Neue PIN ist nicht zu lang
CN-SHORT_PASSWORD-2	Neue PIN ist nicht zu kurz
CN-OBJECT_INITIALIZATION-2	PIN-Objekt befindet sich nicht im Zustand "initialisation"

2.47.4 APDU-Kommandos

ID: CM-CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

2.47.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.47.6 Verifikationen

ID	Beschreibung
VF-CHANGE_REFERENCE_DATA_CHANGE_PIN-2	Die PIN ist gegenüber dem Wert vor Ausführung des Testfalls nicht verändert.

2.48 Testfall: CHANGE REFERENCE DATA zum Wechseln der PIN (TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_3_1)

2.48.1 Informationen

ID	TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_3_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando CHANGE REFERENCE DATA zum Wechseln der PIN nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Nicht erfüllt bedeutet in diesem Testfall, dass der notwendige PACE-Kanal nicht aufgebaut ist. Dazu wird eine Kommandonachricht für CHANGE REFERENCE DATA zum Wechseln der PIN zum Wechseln einer PIN an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.48.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.8.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_02

2.48.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt (PACE-Kanal nicht aufgebaut)
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN-PASSWORD_NOT_FOUND-2	Das PIN-Objekt kann gefunden werden
CN-LONG_PASSWORD-2	Neue PIN ist nicht zu lang
CN-SHORT_PASSWORD-2	Neue PIN ist nicht zu kurz
CN-OBJECT_INITIALIZATION-2	PIN-Objekt befindet sich nicht im Zustand "initialisation"

2.48.4 APDU-Kommandos

ID: CM-CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_3_1						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

2.48.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.48.6 Verifikationen

ID	Beschreibung
VF-CHANGE_REFERENCE_DATA_CHANGE_PIN-2	Die PIN ist gegenüber dem Wert vor Ausführung des Testfalls nicht verändert.

2.49 Testfall: CHANGE REFERENCE DATA zum Wechseln der PIN (TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_3_2)

2.49.1 Informationen

ID	TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_3_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando CHANGE REFERENCE DATA zum Wechseln der PIN nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Nicht erfüllt bedeutet in diesem Testfall, dass die PIN terminiert ist. Dazu wird eine Kommandonachricht für CHANGE REFERENCE DATA zum Wechseln der PIN zum Wechseln einer PIN an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.49.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.8.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_02

2.49.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt (PIN terminiert)
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN-PASSWORD_NOT_FOUND-2	Das PIN-Objekt kann gefunden werden
CN-LONG_PASSWORD-2	Neue PIN ist nicht zu lang
CN-SHORT_PASSWORD-2	Neue PIN ist nicht zu kurz
CN-OBJECT_INITIALIZATION-2	PIN-Objekt befindet sich nicht im Zustand "initialisation"

2.49.4 APDU-Kommandos

ID: CM-CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_3_2						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

2.49.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.49.6 Verifikationen

ID	Beschreibung
VF-CHANGE_REFERENCE_DATA_CHANGE_PIN-2	Die PIN ist gegenüber dem Wert vor Ausführung des Testfalls nicht verändert.

2.50 Testfall: CHANGE REFERENCE DATA zum Wechseln der PIN (TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_4)

2.50.1 Informationen

ID	TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando CHANGE REFERENCE DATA zum Wechseln der PIN nicht erfolgreich durchgeführt werden kann, wenn die neue PIN zu lang ist. Dazu wird eine Kommandonachricht für CHANGE REFERENCE DATA zum Wechseln der PIN zum Wechseln einer PIN an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.50.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.8.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_02

2.50.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-LONG_PASSWORD-1	Neue PIN ist zu lang
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PASSWORD_NOT_FOUND-2	Das PIN-Objekt kann gefunden werden

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN- SHORT_PASSWOR D-2	Neue PIN ist nicht zu kurz
CN- OBJECT_INITIALIZ ATION-2	PIN-Objekt befindet sich nicht im Zustand "initialisation"

2.50.4 APDU-Kommandos

ID: CM-CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_4						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

2.50.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A87	Das Testsystem antwortet mit '6a 87'.

2.50.6 Verifikationen

ID	Beschreibung
VF- CHANGE_REFERENCE_DATA_CHANGE_P IN-2	Die PIN ist gegenüber dem Wert vor Ausführung des Testfalls nicht verändert.

2.51 Testfall: CHANGE REFERENCE DATA zum Wechseln der PIN (TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_5)

2.51.1 Informationen

ID	TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando CHANGE REFERENCE DATA zum Wechseln der PIN nicht erfolgreich durchgeführt werden kann, wenn die neue PIN zu kurz ist. Dazu wird eine Kommandonachricht für CHANGE REFERENCE DATA zum Wechseln der PIN zum Wechseln einer PIN an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.51.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.8.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_02

2.51.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SHORT_PASSWORD-1	Neue PIN ist zu kurz
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PASSWORD_NOT_FOUND-2	Das PIN-Objekt kann gefunden werden

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN- LONG_PASSWORD -2	Neue PIN ist nicht zu lang
CN- OBJECT_INITIALIZ ATION-2	PIN-Objekt befindet sich nicht im Zustand "initialisation"

2.51.4 APDU-Kommandos

ID: CM-CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_5						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

2.51.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A87	Das Testsystem antwortet mit '6a 87'.

2.51.6 Verifikationen

ID	Beschreibung
VF- CHANGE_REFERENCE_DATA_CHANGE_P IN-2	Die PIN ist gegenüber dem Wert vor Ausführung des Testfalls nicht verändert.

2.52 Testfall: CHANGE REFERENCE DATA zum Wechseln der PIN (TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_6)

2.52.1 Informationen

ID	TC_CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando CHANGE REFERENCE DATA zum Wechseln der PIN nicht erfolgreich durchgeführt werden kann, wenn sich das PIN-Objekt im Zustand "initialisation" befindet. Dazu wird eine Kommandonachricht für CHANGE REFERENCE DATA zum Wechseln der PIN zum Wechseln einer PIN an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.52.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.8.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_02

2.52.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_INITIALIZATION-1	PIN-Objekt befindet sich im Zustand "initialisation"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PASSWORD_NOT_	Das PIN-Objekt kann gefunden werden

FOUND-2	
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN- LONG_PASSWORD -2	Neue PIN ist nicht zu lang
CN- SHORT_PASSWOR D-2	Neue PIN ist nicht zu kurz

2.52.4 APDU-Kommandos

ID: CM-CHANGE_REFERENCE_DATA_CHANGE_PIN_FF_6						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

2.52.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.52.6 Verifikationen

ID	Beschreibung
VF- CHANGE_REFERENCE_DATA_CHANGE_P IN-2	Die PIN ist gegenüber dem Wert vor Ausführung des Testfalls nicht verändert.

2.53 Testfall: CHANGE REFERENCE DATA zum Setzen der PIN (TC_CHANGE_REFERENCE_DATA_SET_PIN_GF_1)

2.53.1 Informationen

ID	TC_CHANGE_REFERENCE_DATA_SET_PIN_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando CHANGE REFERENCE DATA zum Setzen der PIN erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für CHANGE REFERENCE DATA zum Setzen der PIN zum Setzen einer PIN an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.53.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.8.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_01

2.53.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PASSWORD_NOT_FOUND-2	Das PIN-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.53.4 APDU-Kommandos

ID: CM-CHANGE_REFERENCE_DATA_SET_PIN_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	24	01	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die neue PIN.

2.53.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.53.6 Verifikationen

ID	Beschreibung
VF- CHANGE_REFERENCE_DATA_SET_PIN-1	Die PIN ist gesetzt.

2.54 Testfall: CHANGE REFERENCE DATA zum Setzen der PIN (TC_CHANGE_REFERENCE_DATA_SET_PIN_FF_1)

2.54.1 Informationen

ID	TC_CHANGE_REFERENCE_DATA_SET_PIN_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando CHANGE REFERENCE DATA zum Setzen der PIN nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für CHANGE REFERENCE DATA zum Setzen der PIN zum Setzen einer PIN an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.54.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.8.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_01

2.54.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-PASSWORD_NOT_FOUND-2	Das PIN-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.54.4 APDU-Kommandos

ID: CM-CHANGE_REFERENCE_DATA_SET_PIN_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	24	01	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die neue PIN.

2.54.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.54.6 Verifikationen

ID	Beschreibung
VF- CHANGE_REFERENCE_DATA_SET_PIN-2	Die PIN ist nicht gesetzt.

2.55 Testfall: CHANGE REFERENCE DATA zum Setzen der PIN (TC_CHANGE_REFERENCE_DATA_SET_PIN_FF_2)

2.55.1 Informationen

ID	TC_CHANGE_REFERENCE_DATA_SET_PIN_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando CHANGE REFERENCE DATA zum Setzen der PIN nicht erfolgreich durchgeführt werden kann, wenn das mittels P2-Parameter adressierte PIN-Objekt nicht gefunden wird. Dazu wird eine Kommandonachricht für CHANGE REFERENCE DATA zum Setzen der PIN zum Setzen einer PIN an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.55.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.8.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_01

2.55.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- PASSWORD_NOT_ FOUND-1	Das PIN-Objekt kann nicht gefunden werden

CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.55.4 APDU-Kommandos

ID: CM-CHANGE_REFERENCE_DATA_SET_PIN_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	24	01	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die neue PIN.

2.55.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.55.6 Verifikationen

ID	Beschreibung
VF-CHANGE_REFERENCE_DATA_SET_PIN-2	Die PIN ist nicht gesetzt.

2.56 Testfall: CHANGE REFERENCE DATA zum Setzen der PIN (TC_CHANGE_REFERENCE_DATA_SET_PIN_FF_3)

2.56.1 Informationen

ID	TC_CHANGE_REFERENCE_DATA_SET_PIN_FF_3

Beschreibung	Dieser Test verifiziert, dass ein Kommando CHANGE REFERENCE DATA zum Setzen der PIN nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Dazu wird eine Kommandonachricht für CHANGE REFERENCE DATA zum Setzen der PIN zum Setzen einer PIN an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.56.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.8.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_01

2.56.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PASSWORD_NOT_FOUND-2	Das PIN-Objekt kann gefunden werden

2.56.4 APDU-Kommandos

ID: CM-CHANGE_REFERENCE_DATA_SET_PIN_FF_3						
CLA	INS	P1	P2	Lc	Data	Le

00	24	01	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die neue PIN.

2.56.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.56.6 Verifikationen

ID	Beschreibung
VF- CHANGE_REFERENCE_DATA_SET_PIN-2	Die PIN ist nicht gesetzt.

2.57 Testfall: CREATE FILE (TC_CREATE_FILE_GF_1)

2.57.1 Informationen

ID	TC_CREATE_FILE_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE FILE erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für CREATE FILE zum Anlegen eines DFs/EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.57.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_17

2.57.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-DF_NAME_EXISTS-2	AID des neuen Objekts wird nicht bereits verwendet
CN-DUPLICATED_OBJECT-2	FID des neuen Objekts wird nicht bereits verwendet
CN-OUT_OF_MEMORY-2	Speicherplatz des Sicherheitsmoduls reicht aus

2.57.4 APDU-Kommandos

ID: CM-CREATE_FILE_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.57.5 Erwartete Ergebnisse

ID	Beschreibung

RS-9000	Das Testsystem antwortet mit '90 00'.

2.57.6 Verifikationen

ID	Beschreibung
VF-CREATE_FILE-1	Das entsprechende File ist auf dem Kartensystem vorhanden und kann erfolgreich selektiert werden.

2.58 Testfall: CREATE FILE (TC_CREATE_FILE_FF_1)

2.58.1 Informationen

ID	TC_CREATE_FILE_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE FILE nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für CREATE FILE zum Anlegen eines DFs/EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.58.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_17

2.58.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-	Sicherheitsmodul befindet sich im Zustand "terminiert"

INSTRUCTION_NO T_SUPPORTED-1	
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN- DF_NAME_EXISTS- 2	AID des neuen Objekts wird nicht bereits verwendet
CN- DUPLICATED_OBJ ECT-2	FID des neuen Objekts wird nicht bereits verwendet
CN- OUT_OF_MEMORY -2	Speicherplatz des Sicherheitsmoduls reicht aus

2.58.4 APDU-Kommandos

ID: CM-CREATE_FILE_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.58.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.58.6 Verifikationen

ID	Beschreibung
VF-CREATE_FILE-2	Das entsprechende File ist auf dem Kartensystem nicht vorhanden und kann daher

	nicht selektiert werden.

2.59 Testfall: CREATE FILE (TC_CREATE_FILE_FF_2)

2.59.1 Informationen

ID	TC_CREATE_FILE_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE FILE nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Dazu wird eine Kommandonachricht für CREATE FILE zum Anlegen eines DFs/EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.59.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_17

2.59.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-	AID des neuen Objekts wird nicht bereits verwendet

DF_NAME_EXISTS-2	
CN-DUPLICATED_OBJECT-2	FID des neuen Objekts wird nicht bereits verwendet
CN-OUT_OF_MEMORY-2	Speicherplatz des Sicherheitsmoduls reicht aus

2.59.4 APDU-Kommandos

ID: CM-CREATE_FILE_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.59.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.59.6 Verifikationen

ID	Beschreibung
VF-CREATE_FILE-2	Das entsprechende File ist auf dem Kartensystem nicht vorhanden und kann daher nicht selektiert werden.

2.60 Testfall: CREATE FILE (TC_CREATE_FILE_FF_3)

2.60.1 Informationen

ID	TC_CREATE_FILE_FF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE FILE nicht erfolgreich durchgeführt werden kann, wenn der AID des neuen Objekts bereits verwendet wird. Dazu wird eine Kommandonachricht für CREATE FILE zum Anlegen eines DFs/EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.60.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_17

2.60.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-DF_NAME_EXISTS-1	AID des neuen Objekts wird bereits verwendet
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-	FID des neuen Objekts wird nicht bereits verwendet

DUPLICATED_OBJECT-2	
CN-OUT_OF_MEMORY-2	Speicherplatz des Sicherheitsmoduls reicht aus

2.60.4 APDU-Kommandos

ID: CM-CREATE_FILE_FF_3						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.60.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A8A	Das Testsystem antwortet mit '6a 8a'.

2.60.6 Verifikationen

ID	Beschreibung
VF-CREATE_FILE-2	Das entsprechende File ist auf dem Kartensystem nicht vorhanden und kann daher nicht selektiert werden.

2.61 Testfall: CREATE FILE (TC_CREATE_FILE_FF_4)

2.61.1 Informationen

ID	TC_CREATE_FILE_FF_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE FILE nicht erfolgreich durchgeführt werden kann, wenn der FID des neuen Objekts

	bereits verwendet wird. Dazu wird eine Kommandonachricht für CREATE FILE zum Anlegen eines DFs/EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.61.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_17

2.61.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-DUPLICATED_OBJECT-1	FID des neuen Objekts wird bereits verwendet
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-DF_NAME_EXISTS-2	AID des neuen Objekts wird nicht bereits verwendet
CN-OUT_OF_MEMORY-2	Speicherplatz des Sicherheitsmoduls reicht aus

2.61.4 APDU-Kommandos

ID: CM-CREATE_FILE_FF_4						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.61.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A89	Das Testsystem antwortet mit '6a 89'.

2.61.6 Verifikationen

ID	Beschreibung
VF-CREATE_FILE-2	Das entsprechende File ist auf dem Kartensystem nicht vorhanden und kann daher nicht selektiert werden.

2.62 Testfall: CREATE FILE (TC_CREATE_FILE_FF_5)

2.62.1 Informationen

ID	TC_CREATE_FILE_FF_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE FILE nicht erfolgreich durchgeführt werden kann, wenn der restliche Speicherplatz des Sicherheitsmoduls nicht ausreicht. Dazu wird eine Kommandonachricht für CREATE FILE zum Anlegen eines DFs/EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.62.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_17

2.62.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OUT_OF_MEMORY-1	Speicherplatz des Sicherheitsmoduls reicht nicht aus
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-DF_NAME_EXISTS-2	AID des neuen Objekts wird nicht bereits verwendet
CN-DUPLICATED_OBJECT-2	FID des neuen Objekts wird nicht bereits verwendet

2.62.4 APDU-Kommandos

ID: CM-CREATE_FILE_FF_5						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.62.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A84	Das Testsystem antwortet mit '6a 84'.

2.62.6 Verifikationen

ID	Beschreibung
VF-CREATE_FILE-2	Das entsprechende File ist auf dem Kartensystem nicht vorhanden und kann daher nicht selektiert werden.

2.63 Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_1)

2.63.1 Informationen

ID	TC_CREATE_KEY_GF_1_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein DST (ECDSA mit SHA1) für Public-Key-Objekt. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.63.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.63.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-DUPLICATED_OBJECT-2	KID des neuen Objekts wird nicht bereits verwendet
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN-OUT_OF_MEMORY-2	Speicherplatz des Sicherheitsmoduls reicht aus

2.63.4 APDU-Kommandos

ID: CM-CREATE_KEY_GF_1_1						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	62 LL [ad LL [83 LL [XX...XX] 96 LL [XX...XX] a2 00]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.63.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.63.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-1	Das entsprechende Key-Objekt ist auf dem Kartensystem vorhanden und kann selektiert werden.

2.64 Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_2)

2.64.1 Informationen

ID	TC_CREATE_KEY_GF_1_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein DST (ECDSA mit SHA256) für Public-Key-Objekt. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.64.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.64.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN- DUPLICATED_OBJ ECT-2	KID des neuen Objekts wird nicht bereits verwendet
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN- OUT_OF_MEMORY -2	Speicherplatz des Sicherheitsmoduls reicht aus

2.64.4 APDU-Kommandos

ID: CM-CREATE_KEY_GF_1_2						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	62 LL [ad LL [83 LL [XX...XX] 96 LL [XX...XX] a2 00]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.64.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.64.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-1	Das entsprechende Key-Objekt ist auf dem Kartensystem vorhanden und kann selektiert werden.

2.65 Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_3)

2.65.1 Informationen

ID	TC_CREATE_KEY_GF_1_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein DST (ECDSA mit SH384) für Public-Key-Objekt. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.65.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.65.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-DUPLICATED_OBJECT-2	KID des neuen Objekts wird nicht bereits verwendet

CN- INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN- OUT_OF_MEMORY-2	Speicherplatz des Sicherheitsmoduls reicht aus

2.65.4 APDU-Kommandos

ID: CM-CREATE_KEY_GF_1_3						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	62 LL [ad LL [83 LL [XX...XX] 96 LL [XX...XX] a2 00]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.65.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.65.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-1	Das entsprechende Key-Objekt ist auf dem Kartensystem vorhanden und kann selektiert werden.

2.66 Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_4)

2.66.1 Informationen

ID	TC_CREATE_KEY_GF_1_4

Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein DST (ECDSA mit SH512) für Public-Key-Objekt. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.66.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.66.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-DUPLICATED_OBJECT-2	KID des neuen Objekts wird nicht bereits verwendet
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN-OUT_OF_MEMORY-2	Speicherplatz des Sicherheitsmoduls reicht aus

2.66.4 APDU-Kommandos

ID: CM-CREATE_KEY_GF_1_4						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	62 LL [ad LL [83 LL [XX...XX] 96 LL [XX...XX] a2 00]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.66.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.66.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-1	Das entsprechende Key-Objekt ist auf dem Kartensystem vorhanden und kann selektiert werden.

2.67 Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_5)

2.67.1 Informationen

ID	TC_CREATE_KEY_GF_1_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein DST (ECDSA ohne Hashing) für Public-Key-Objekt. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.

Klassifizierung	Gutfall-Test

2.67.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.67.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-DUPLICATED_OBJECT-2	KID des neuen Objekts wird nicht bereits verwendet
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN-OUT_OF_MEMORY-2	Speicherplatz des Sicherheitsmoduls reicht aus

2.67.4 APDU-Kommandos

ID: CM-CREATE_KEY_GF_1_5						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	62 LL [ad LL [83 LL [XX...XX] 96 LL	--

					[XX...XX] a2 00]]	

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.67.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.67.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-1	Das entsprechende Key-Objekt ist auf dem Kartensystem vorhanden und kann selektiert werden.

2.68 Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_6)

2.68.1 Informationen

ID	TC_CREATE_KEY_GF_1_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein AT (ECDSA mit SHA256) für Public-Key-Objekt. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.68.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.68.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN- DUPLICATED_OBJ ECT-2	KID des neuen Objekts wird nicht bereits verwendet
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN- OUT_OF_MEMORY -2	Speicherplatz des Sicherheitsmoduls reicht aus

2.68.4 APDU-Kommandos

ID: CM-CREATE_KEY_GF_1_6						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	62 LL [ad LL [83 LL [XX...XX] 96 LL [XX...XX] a2 00]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.68.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.68.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-1	Das entsprechende Key-Objekt ist auf dem Kartensystem vorhanden und kann selektiert werden.

2.69 Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_7)

2.69.1 Informationen

ID	TC_CREATE_KEY_GF_1_7
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein AT (ECDSA mit SH384) für Public-Key-Objekt. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.69.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.69.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN- DUPLICATED_OBJ ECT-2	KID des neuen Objekts wird nicht bereits verwendet
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN- OUT_OF_MEMORY -2	Speicherplatz des Sicherheitsmoduls reicht aus

2.69.4 APDU-Kommandos

ID: CM-CREATE_KEY_GF_1_7						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	62 LL [ad LL [83 LL [XX...XX] 96 LL [XX...XX] a2 00]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.69.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.69.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-1	Das entsprechende Key-Objekt ist auf dem Kartensystem vorhanden und kann selektiert werden.

2.70 Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_8)

2.70.1 Informationen

ID	TC_CREATE_KEY_GF_1_8
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein AT (ECDSA mit SH512) für Public-Key-Objekt. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.70.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.70.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN- DUPLICATED_OBJ ECT-2	KID des neuen Objekts wird nicht bereits verwendet
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN- OUT_OF_MEMORY -2	Speicherplatz des Sicherheitsmoduls reicht aus

2.70.4 APDU-Kommandos

ID: CM-CREATE_KEY_GF_1_8						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	62 LL [ad LL [83 LL [XX...XX] 96 LL [XX...XX] a2 00]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.70.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.70.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-1	Das entsprechende Key-Objekt ist auf dem Kartensystem vorhanden und kann selektiert werden.

2.71 Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_9)

2.71.1 Informationen

ID	TC_CREATE_KEY_GF_1_9
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein AT (ECKA-EG) für Public-Key-Objekt. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.71.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.71.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-DUPLICATED_OBJECT-2	KID des neuen Objekts wird nicht bereits verwendet

CN- INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN- OUT_OF_MEMORY-2	Speicherplatz des Sicherheitsmoduls reicht aus

2.71.4 APDU-Kommandos

ID: CM-CREATE_KEY_GF_1_9						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	62 LL [ad LL [83 LL [XX...XX] 96 LL [XX...XX] a2 00]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.71.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.71.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-1	Das entsprechende Key-Objekt ist auf dem Kartensystem vorhanden und kann selektiert werden.

2.72 Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_10)

2.72.1 Informationen

ID	TC_CREATE_KEY_GF_1_10

Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein AT (ECKA-DH) für Public-Key-Objekt. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.72.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.72.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-DUPLICATED_OBJECT-2	KID des neuen Objekts wird nicht bereits verwendet
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN-OUT_OF_MEMORY-2	Speicherplatz des Sicherheitsmoduls reicht aus

2.72.4 APDU-Kommandos

ID: CM-CREATE_KEY_GF_1_10						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	62 LL [ad LL [83 LL [XX...XX] 96 LL [XX...XX] a2 00]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.72.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.72.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-1	Das entsprechende Key-Objekt ist auf dem Kartensystem vorhanden und kann selektiert werden.

2.73 Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_11)

2.73.1 Informationen

ID	TC_CREATE_KEY_GF_1_11
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein DST (ECDSA ohne Hashing) für Key-Pair-Objekt. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.

Klassifizierung	Gutfall-Test

2.73.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.73.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-DUPLICATED_OBJECT-2	KID des neuen Objekts wird nicht bereits verwendet
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN-OUT_OF_MEMORY-2	Speicherplatz des Sicherheitsmoduls reicht aus

2.73.4 APDU-Kommandos

ID: CM-CREATE_KEY_GF_1_11						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	62 LL [ad LL [83 LL [XX...XX] 96 LL	--

					[XX...XX] a1 00]]	

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.73.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.73.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-1	Das entsprechende Key-Objekt ist auf dem Kartensystem vorhanden und kann selektiert werden.

2.74 Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_12)

2.74.1 Informationen

ID	TC_CREATE_KEY_GF_1_12
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein AT (ECDSA ohne Hashing) für Key-Pair-Objekt. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.74.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.74.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-DUPLICATED_OBJECT-2	KID des neuen Objekts wird nicht bereits verwendet
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN-OUT_OF_MEMORY-2	Speicherplatz des Sicherheitsmoduls reicht aus

2.74.4 APDU-Kommandos

ID: CM-CREATE_KEY_GF_1_12						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	62 LL [ad LL [83 LL [XX...XX] 96 LL [XX...XX] a1 00]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.74.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.74.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-1	Das entsprechende Key-Objekt ist auf dem Kartensystem vorhanden und kann selektiert werden.

2.75 Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_13)

2.75.1 Informationen

ID	TC_CREATE_KEY_GF_1_13
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein AT (ECKA-EG) für Key-Pair-Objekt. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.75.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.75.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN- DUPLICATED_OBJ ECT-2	KID des neuen Objekts wird nicht bereits verwendet
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN- OUT_OF_MEMORY -2	Speicherplatz des Sicherheitsmoduls reicht aus

2.75.4 APDU-Kommandos

ID: CM-CREATE_KEY_GF_1_13						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	62 LL [ad LL [83 LL [XX...XX] 96 LL [XX...XX] a1 00]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.75.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.75.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-1	Das entsprechende Key-Objekt ist auf dem Kartensystem vorhanden und kann selektiert werden.

2.76 Testfall: CREATE KEY (TC_CREATE_KEY_GF_1_14)

2.76.1 Informationen

ID	TC_CREATE_KEY_GF_1_14
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein AT (ECKA-DH) für Key-Pair-Objekt. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.76.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.76.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN- DUPLICATED_OBJ ECT-2	KID des neuen Objekts wird nicht bereits verwendet
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN- OUT_OF_MEMORY -2	Speicherplatz des Sicherheitsmoduls reicht aus

2.76.4 APDU-Kommandos

ID: CM-CREATE_KEY_GF_1_14						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	62 LL [ad LL [83 LL [XX...XX] 96 LL [XX...XX] a1 00]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.76.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.76.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-1	Das entsprechende Key-Objekt ist auf dem Kartensystem vorhanden und kann selektiert werden.

2.77 Testfall: CREATE KEY (TC_CREATE_KEY_FF_1)

2.77.1 Informationen

ID	TC_CREATE_KEY_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.77.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.77.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-DUPLICATED_OBJECT-2	KID des neuen Objekts wird nicht bereits verwendet
CN-	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt

INCORRECT_PARAMETERS-2	vorhandenes Datenobjekt für AT)
CN-OUT_OF_MEMORY-2	Speicherplatz des Sicherheitsmoduls reicht aus

2.77.4 APDU-Kommandos

ID: CM-CREATE_KEY_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.77.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.77.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-2	Das entsprechende Key-Objekt ist auf dem Kartensystem nicht vorhanden und kann daher nicht selektiert werden.

2.78 Testfall: CREATE KEY (TC_CREATE_KEY_FF_2_1)

2.78.1 Informationen

ID	TC_CREATE_KEY_FF_2_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext

	des Objekts nicht erfüllt sind. Nicht erfüllt bedeutet in diesem Testfall, dass eine notwendige Authentifizierung fehlt. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.78.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.78.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt (Authentifizierung nicht durchgeführt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-DUPLICATED_OBJECT-2	KID des neuen Objekts wird nicht bereits verwendet
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN-OUT_OF_MEMORY-2	Speicherplatz des Sicherheitsmoduls reicht aus

2.78.4 APDU-Kommandos

ID: CM-CREATE_KEY_FF_2_1						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.78.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.78.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-2	Das entsprechende Key-Objekt ist auf dem Kartensystem nicht vorhanden und kann daher nicht selektiert werden.

2.79 Testfall: CREATE KEY (TC_CREATE_KEY_FF_2_2)

2.79.1 Informationen

ID	TC_CREATE_KEY_FF_2_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Nicht erfüllt bedeutet in diesem Testfall, dass der notwendige PACE-Kanal nicht aufgebaut ist. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.

Klassifizierung	Fehlerfall-Test

2.79.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.79.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt (PACE-Kanal nicht aufgebaut)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-DUPLICATED_OBJECT-2	KID des neuen Objekts wird nicht bereits verwendet
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN-OUT_OF_MEMORY-2	Speicherplatz des Sicherheitsmoduls reicht aus

2.79.4 APDU-Kommandos

ID: CM-CREATE_KEY_FF_2_2						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.79.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.79.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-2	Das entsprechende Key-Objekt ist auf dem Kartensystem nicht vorhanden und kann daher nicht selektiert werden.

2.80 Testfall: CREATE KEY (TC_CREATE_KEY_FF_3)

2.80.1 Informationen

ID	TC_CREATE_KEY_FF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY nicht erfolgreich durchgeführt werden kann, wenn der KID des neuen Objekts bereits verwendet wird. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.80.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.80.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-DUPLICATED_OBJECT-1	KID des neuen Objekts wird bereits verwendet
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)
CN-OUT_OF_MEMORY-2	Speicherplatz des Sicherheitsmoduls reicht aus

2.80.4 APDU-Kommandos

ID: CM-CREATE_KEY_FF_3						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.80.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A89	Das Testsystem antwortet mit '6a 89'.

2.80.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-2	Das entsprechende Key-Objekt ist auf dem Kartensystem nicht vorhanden und kann daher nicht selektiert werden.

2.81 Testfall: CREATE KEY (TC_CREATE_KEY_FF_4_1)

2.81.1 Informationen

ID	TC_CREATE_KEY_FF_4_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt für AT doppelt vorhanden ist. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.81.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.81.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- INCORRECT_PARA METERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Doppelt vorhandenes Datenobjekt für AT)
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN- DUPLICATED_OBJ ECT-2	KID des neuen Objekts wird nicht bereits verwendet
CN- OUT_OF_MEMORY -2	Speicherplatz des Sicherheitsmoduls reicht aus

2.81.4 APDU-Kommandos

ID: CM-CREATE_KEY_FF_4_1						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.81.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.81.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-2	Das entsprechende Key-Objekt ist auf dem Kartensystem nicht vorhanden und kann daher nicht selektiert werden.

2.82 Testfall: CREATE KEY (TC_CREATE_KEY_FF_4_2)

2.82.1 Informationen

ID	TC_CREATE_KEY_FF_4_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt für DST doppelt vorhanden ist. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.82.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.82.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETER	Parameter im Kommando-Datenfeld sind nicht korrekt (Doppelt vorhandenes Datenobjekt für DST)

METERS-1	
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-DUPLICATED_OBJECT-2	KID des neuen Objekts wird nicht bereits verwendet
CN-OUT_OF_MEMORY-2	Speicherplatz des Sicherheitsmoduls reicht aus

2.82.4 APDU-Kommandos

ID: CM-CREATE_KEY_FF_4_2						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.82.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.82.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-2	Das entsprechende Key-Objekt ist auf dem Kartensystem nicht vorhanden und kann daher nicht selektiert werden.

2.83 Testfall: CREATE KEY (TC_CREATE_KEY_FF_4_3)

2.83.1 Informationen

ID	TC_CREATE_KEY_FF_4_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt für AT ein falsches Tag besitzt. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.83.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.83.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für AT)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUS_NOT_SATISFIED-	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2	
CN-DUPLICATED_OBJECT-2	KID des neuen Objekts wird nicht bereits verwendet
CN-OUT_OF_MEMORY-2	Speicherplatz des Sicherheitsmoduls reicht aus

2.83.4 APDU-Kommandos

ID: CM-CREATE_KEY_FF_4_3						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.83.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.83.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-2	Das entsprechende Key-Objekt ist auf dem Kartensystem nicht vorhanden und kann daher nicht selektiert werden.

2.84 Testfall: CREATE KEY (TC_CREATE_KEY_FF_4_4)

2.84.1 Informationen

ID	TC_CREATE_KEY_FF_4_4

Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt für DST ein falsches Tag besitzt. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.84.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.84.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für DST)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-DUPLICATED_OBJECT-2	KID des neuen Objekts wird nicht bereits verwendet
CN-OUT_OF_MEMORY	Speicherplatz des Sicherheitsmoduls reicht aus

-2

2.84.4 APDU-Kommandos

ID: CM-CREATE_KEY_FF_4_4						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.84.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.84.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-2	Das entsprechende Key-Objekt ist auf dem Kartensystem nicht vorhanden und kann daher nicht selektiert werden.

2.85 Testfall: CREATE KEY (TC_CREATE_KEY_FF_4_5)

2.85.1 Informationen

ID	TC_CREATE_KEY_FF_4_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt für das Key-Pair-Objekt ein falsches Tag besitzt. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die

	inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.85.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.85.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für das Key-Pair-Objekt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-DUPLICATED_OBJECT-2	KID des neuen Objekts wird nicht bereits verwendet
CN-OUT_OF_MEMORY-2	Speicherplatz des Sicherheitsmoduls reicht aus

2.85.4 APDU-Kommandos

ID: CM-CREATE_KEY_FF_4_5

CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.85.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.85.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-2	Das entsprechende Key-Objekt ist auf dem Kartensystem nicht vorhanden und kann daher nicht selektiert werden.

2.86 Testfall: CREATE KEY (TC_CREATE_KEY_FF_4_6)

2.86.1 Informationen

ID	TC_CREATE_KEY_FF_4_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt für das Public-Key-Objekt ein falsches Tag besitzt. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.86.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.86.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für das Public-Key-Objekt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-DUPLICATED_OBJECT-2	KID des neuen Objekts wird nicht bereits verwendet
CN-OUT_OF_MEMORY-2	Speicherplatz des Sicherheitsmoduls reicht aus

2.86.4 APDU-Kommandos

ID: CM-CREATE_KEY_FF_4_6						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.86.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.86.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-2	Das entsprechende Key-Objekt ist auf dem Kartensystem nicht vorhanden und kann daher nicht selektiert werden.

2.87 Testfall: CREATE KEY (TC_CREATE_KEY_FF_4_7)

2.87.1 Informationen

ID	TC_CREATE_KEY_FF_4_7
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt einen zu langen Key-Namen für das Key-Pair-Objekt besitzt. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.87.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.87.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit zu langen Key-Namen für null)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-DUPLICATED_OBJECT-2	KID des neuen Objekts wird nicht bereits verwendet
CN-OUT_OF_MEMORY-2	Speicherplatz des Sicherheitsmoduls reicht aus

2.87.4 APDU-Kommandos

ID: CM-CREATE_KEY_FF_4_7						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.87.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.87.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-2	Das entsprechende Key-Objekt ist auf dem Kartensystem nicht vorhanden und kann daher nicht selektiert werden.

2.88 Testfall: CREATE KEY (TC_CREATE_KEY_FF_4_8)

2.88.1 Informationen

ID	TC_CREATE_KEY_FF_4_8
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt einen zu langen Key-Namen für das Public-Key-Objekt besitzt. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.88.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.88.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- INCORRECT_PARA METERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit zu langen Key-Namen für null)
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN- DUPLICATED_OBJ ECT-2	KID des neuen Objekts wird nicht bereits verwendet
CN- OUT_OF_MEMORY -2	Speicherplatz des Sicherheitsmoduls reicht aus

2.88.4 APDU-Kommandos

ID: CM-CREATE_KEY_FF_4_8						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.88.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.88.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-2	Das entsprechende Key-Objekt ist auf dem Kartensystem nicht vorhanden und kann daher nicht selektiert werden.

2.89 Testfall: CREATE KEY (TC_CREATE_KEY_FF_5)

2.89.1 Informationen

ID	TC_CREATE_KEY_FF_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando CREATE KEY nicht erfolgreich durchgeführt werden kann, wenn der restliche Speicherplatz des Sicherheitsmoduls nicht ausreicht. Dazu wird eine Kommandonachricht für CREATE KEY zum Anlegen eines leeren, persistent gespeicherten Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.89.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_05

2.89.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OUT_OF_MEMORY-1	Speicherplatz des Sicherheitsmoduls reicht nicht aus

CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-DUPLICATED_OBJECT-2	KID des neuen Objekts wird nicht bereits verwendet
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)

2.89.4 APDU-Kommandos

ID: CM-CREATE_KEY_FF_5						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

2.89.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A84	Das Testsystem antwortet mit '6a 84'.

2.89.6 Verifikationen

ID	Beschreibung
VF-CREATE_KEY-2	Das entsprechende Key-Objekt ist auf dem Kartensystem nicht vorhanden und kann daher nicht selektiert werden.

2.90 Testfall: DEACTIVATE FILE (TC_DEACTIVATE_FILE_GF_1)

2.90.1 Informationen

ID	TC_DEACTIVATE_FILE_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando DEACTIVATE FILE erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für DEACTIVATE FILE zur Deaktivierung eines DFs/EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.90.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_20a

2.90.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-CURRENT_FILE-2	Das File ist ausgewählt
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

CN- OBJECT_TERMINATED-2	Objekt befindet sich nicht im Zustand "terminated"

2.90.4 APDU-Kommandos

ID: CM-DEACTIVATE_FILE_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	00	00	--	--	--

2.90.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.90.6 Verifikationen

ID	Beschreibung
VF-DEACTIVATE_FILE-1	Das entsprechende File ist nicht auslesbar.

2.91 Testfall: DEACTIVATE FILE (TC_DEACTIVATE_FILE_FF_1)

2.91.1 Informationen

ID	TC_DEACTIVATE_FILE_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando DEACTIVATE FILE nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für DEACTIVATE FILE zur Deaktivierung eines DFs/EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.91.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_20a

2.91.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-NO_CURRENT_FILE-2	Das File ist ausgewählt
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_TERMINATED-2	Objekt befindet sich nicht im Zustand "terminated"

2.91.4 APDU-Kommandos

ID: CM-DEACTIVATE_FILE_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	00	00	--	--	--

2.91.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.91.6 Verifikationen

ID	Beschreibung
VF-DEACTIVATE_FILE-2	Das entsprechende File ist erfolgreich auslesbar.

2.92 Testfall: DEACTIVATE FILE (TC_DEACTIVATE_FILE_FF_2)

2.92.1 Informationen

ID	TC_DEACTIVATE_FILE_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando DEACTIVATE FILE nicht durchführen lässt, wenn das File vorher nicht selektiert wurde. Dazu wird eine Kommandonachricht für DEACTIVATE FILE zur Deaktivierung eines DFs/EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.92.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_20a

2.92.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-NO_CURRENT_FILE-1	Das File ist nicht ausgewählt
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN- OBJECT_TERMINA TED-2	Objekt befindet sich nicht im Zustand "terminated"

2.92.4 APDU-Kommandos

ID: CM-DEACTIVATE_FILE_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	00	00	--	--	--

2.92.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6986	Das Testsystem antwortet mit '69 86'.

2.92.6 Verifikationen

ID	Beschreibung
VF-DEACTIVATE_FILE-2	Das entsprechende File ist erfolgreich auslesbar.

2.93 Testfall: DEACTIVATE FILE (TC_DEACTIVATE_FILE_FF_3)

2.93.1 Informationen

ID	TC_DEACTIVATE_FILE_FF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando DEACTIVATE FILE nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Dazu wird eine Kommandonachricht für

	DEACTIVATE FILE zur Deaktivierung eines DFs/EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.93.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_20a

2.93.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-CURRENT_FILE-2	Das File ist ausgewählt
CN-OBJECT_TERMINATED-2	Objekt befindet sich nicht im Zustand "terminated"

2.93.4 APDU-Kommandos

ID: CM-DEACTIVATE_FILE_FF_3						
CLA	INS	P1	P2	Lc	Data	Le

00	a4	00	00	--	--	--

2.93.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.93.6 Verifikationen

ID	Beschreibung
VF-DEACTIVATE_FILE-2	Das entsprechende File ist erfolgreich auslesbar.

2.94 Testfall: DEACTIVATE FILE (TC_DEACTIVATE_FILE_FF_4)

2.94.1 Informationen

ID	TC_DEACTIVATE_FILE_FF_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando DEACTIVATE FILE nicht erfolgreich durchgeführt werden kann, wenn sich das Objekt im Zustand "terminated" befindet. Dazu wird eine Kommandonachricht für DEACTIVATE FILE zur Deaktivierung eines DFs/EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.94.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_20a

2.94.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_TERMINATED-1	Objekt befindet sich im Zustand "terminated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_CURRENT_FILE-2	Das File ist ausgewählt
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.94.4 APDU-Kommandos

ID: CM-DEACTIVATE_FILE_FF_4						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	00	00	--	--	--

2.94.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.94.6 Verifikationen

ID	Beschreibung
VF-DEACTIVATE_FILE-2	Das entsprechende File ist erfolgreich auslesbar.

2.95 Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_GF_1_1)

2.95.1 Informationen

ID	TC_DEACTIVATE_KEY_GF_1_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando DEACTIVATE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Key-Objekt ist in diesem Fall ein Public-Key-Objekt für AT. Dazu wird eine Kommandonachricht für DEACTIVATE KEY zum Deaktivieren eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.95.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_04, PN_04_08

2.95.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2	
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)

2.95.4 APDU-Kommandos

ID: CM-DEACTIVATE_KEY_GF_1_1						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	a4 LL [83 LL [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.95.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.95.6 Verifikationen

ID	Beschreibung
VF-DEACTIVATE_KEY-1	Das entsprechende Key-Objekt ist nicht auslesbar.

2.96 Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_GF_1_2)

2.96.1 Informationen

ID	TC_DEACTIVATE_KEY_GF_1_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando DEACTIVATE KEY

	erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Key-Objekt ist in diesem Fall ein Public-Key-Objekt für DST. Dazu wird eine Kommandonachricht für DEACTIVATE KEY zum Deaktivieren eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.96.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_04, PN_04_08

2.96.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)

2.96.4 APDU-Kommandos

ID: CM-DEACTIVATE_KEY_GF_1_2

CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	b6 LL [83 LL [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.96.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.96.6 Verifikationen

ID	Beschreibung
VF-DEACTIVATE_KEY-1	Das entsprechende Key-Objekt ist nicht auslesbar.

2.97 Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_GF_1_3)

2.97.1 Informationen

ID	TC_DEACTIVATE_KEY_GF_1_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando DEACTIVATE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Key-Objekt ist in diesem Fall ein Public-Key-Objekt für AT. Dazu wird eine Kommandonachricht für DEACTIVATE KEY zum Deaktivieren eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.97.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_04, PN_04_08

2.97.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)

2.97.4 APDU-Kommandos

ID: CM-DEACTIVATE_KEY_GF_1_3						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	a4 LL [84 01 [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.97.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.97.6 Verifikationen

ID	Beschreibung
VF-DEACTIVATE_KEY-1	Das entsprechende Key-Objekt ist nicht auslesbar.

2.98 Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_GF_1_4)

2.98.1 Informationen

ID	TC_DEACTIVATE_KEY_GF_1_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando DEACTIVATE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Key-Objekt ist in diesem Fall ein Public-Key-Objekt für DST. Dazu wird eine Kommandonachricht für DEACTIVATE KEY zum Deaktivieren eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.98.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_04, PN_04_08

2.98.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)

2.98.4 APDU-Kommandos

ID: CM-DEACTIVATE_KEY_GF_1_4						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	b6 LL [84 01 [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.98.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.98.6 Verifikationen

ID	Beschreibung

VF-DEACTIVATE_KEY-1	Das entsprechende Key-Objekt ist nicht auslesbar.

2.99 Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_1)

2.99.1 Informationen

ID	TC_DEACTIVATE_KEY_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando DEACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für DEACTIVATE KEY zum Deaktivieren eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.99.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_04, PN_04_08

2.99.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)

2.99.4 APDU-Kommandos

ID: CM-DEACTIVATE_KEY_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	a4 LL [83 LL [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.99.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.99.6 Verifikationen

ID	Beschreibung
VF-DEACTIVATE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich auslesbar.

2.100 Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_2_1)

2.100.1 Informationen

ID	TC_DEACTIVATE_KEY_FF_2_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando DEACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn das Public-Key-Objekt für AT nicht gefunden wird. Dazu wird eine Kommandonachricht für DEACTIVATE KEY zum Deaktivieren eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.100.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_04, PN_04_08

2.100.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- KEY_NOT_FOUND- 1	Public-Key-Objekt für AT kann nicht gefunden werden
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

CN- INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)

2.100.4 APDU-Kommandos

ID: CM-DEACTIVATE_KEY_FF_2_1						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	a4 LL [83 LL [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.100.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.100.6 Verifikationen

ID	Beschreibung
VF-DEACTIVATE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich auslesbar.

2.101 Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_2_2)

2.101.1 Informationen

ID	TC_DEACTIVATE_KEY_FF_2_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando DEACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn das Public-Key-Objekt für DST nicht gefunden wird. Dazu wird eine Kommandonachricht für

	DEACTIVATE KEY zum Deaktivieren eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.101.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_04, PN_04_08

2.101.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	Public-Key-Objekt für DST kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)

2.101.4 APDU-Kommandos

ID: CM-DEACTIVATE_KEY_FF_2_2							
CLA	INS	P1	P2	Lc	Data	Le	

00	04	21	00	LL	b6 LL [83 LL [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.101.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.101.6 Verifikationen

ID	Beschreibung
VF-DEACTIVATE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich auslesbar.

2.102 Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_2_3)

2.102.1 Informationen

ID	TC_DEACTIVATE_KEY_FF_2_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando DEACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn das Key-Pair-Objekt für AT nicht gefunden wird. Dazu wird eine Kommandonachricht für DEACTIVATE KEY zum Deaktivieren eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.102.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_04, PN_04_08

2.102.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	Key-Pair-Objekt für AT kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)

2.102.4 APDU-Kommandos

ID: CM-DEACTIVATE_KEY_FF_2_3						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	a4 LL [84 01 [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.102.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.102.6 Verifikationen

ID	Beschreibung
VF-DEACTIVATE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich auslesbar.

2.103 Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_2_4)

2.103.1 Informationen

ID	TC_DEACTIVATE_KEY_FF_2_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando DEACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn das Key-Pair-Objekt für DST nicht gefunden wird. Dazu wird eine Kommandonachricht für DEACTIVATE KEY zum Deaktivieren eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.103.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_04, PN_04_08

2.103.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-	Key-Pair-Objekt für DST kann nicht gefunden werden

KEY_NOT_FOUND-1	
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)

2.103.4 APDU-Kommandos

ID: CM-DEACTIVATE_KEY_FF_2_4						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	b6 LL [84 01 [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.103.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.103.6 Verifikationen

ID	Beschreibung
VF-DEACTIVATE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich auslesbar.

2.104 Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_3_1)

2.104.1 Informationen

ID	TC_DEACTIVATE_KEY_FF_3_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando DEACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Nicht erfüllt bedeutet in diesem Testfall, dass eine notwendige Authentifizierung fehlt. Dazu wird eine Kommandonachricht für DEACTIVATE KEY zum Deaktivieren eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.104.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_04, PN_04_08

2.104.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt (Authentifizierung nicht durchgeführt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-	Key-Pair-Objekt kann gefunden werden

2	
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)

2.104.4 APDU-Kommandos

ID: CM-DEACTIVATE_KEY_FF_3_1						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	a4 LL [83 LL [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.104.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.104.6 Verifikationen

ID	Beschreibung
VF-DEACTIVATE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich auslesbar.

2.105 Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_3_2)

2.105.1 Informationen

ID	TC_DEACTIVATE_KEY_FF_3_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando DEACTIVATE KEY nicht

	erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Nicht erfüllt bedeutet in diesem Testfall, dass der notwendige PACE-Kanal nicht aufgebaut ist. Dazu wird eine Kommandonachricht für DEACTIVATE KEY zum Deaktivieren eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.105.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_04, PN_04_08

2.105.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt (PACE-Kanal nicht aufgebaut)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)

2.105.4 APDU-Kommandos

ID: CM-DEACTIVATE_KEY_FF_3_2

CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	a4 LL [83 LL [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.105.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.105.6 Verifikationen

ID	Beschreibung
VF-DEACTIVATE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich auslesbar.

2.106 Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_4_1)

2.106.1 Informationen

ID	TC_DEACTIVATE_KEY_FF_4_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando DEACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt für AT doppelt vorhanden ist. Dazu wird eine Kommandonachricht für DEACTIVATE KEY zum Deaktivieren eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.106.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_04, PN_04_08

2.106.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Doppelt vorhandenes Datenobjekt für AT)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.106.4 APDU-Kommandos

ID: CM-DEACTIVATE_KEY_FF_4_1						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	a4 LL [83 LL [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.106.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.106.6 Verifikationen

ID	Beschreibung
VF-DEACTIVATE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich auslesbar.

2.107 Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_4_2)

2.107.1 Informationen

ID	TC_DEACTIVATE_KEY_FF_4_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando DEACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt für DST doppelt vorhanden ist. Dazu wird eine Kommandonachricht für DEACTIVATE KEY zum Deaktivieren eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.107.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_04, PN_04_08

2.107.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Doppelt vorhandenes Datenobjekt für DST)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.107.4 APDU-Kommandos

ID: CM-DEACTIVATE_KEY_FF_4_2						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	b6 LL [83 LL [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.107.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.107.6 Verifikationen

ID	Beschreibung

VF-DEACTIVATE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich auslesbar.

2.108 Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_4_3)

2.108.1 Informationen

ID	TC_DEACTIVATE_KEY_FF_4_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando DEACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt für AT ein falsches Tag besitzt. Dazu wird eine Kommandonachricht für DEACTIVATE KEY zum Deaktivieren eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.108.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_04, PN_04_08

2.108.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für AT)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATU S_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.108.4 APDU-Kommandos

ID: CM-DEACTIVATE_KEY_FF_4_3						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	a4 LL [83 LL [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.108.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.108.6 Verifikationen

ID	Beschreibung
VF-DEACTIVATE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich auslesbar.

2.109 Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_4_4)

2.109.1 Informationen

ID	TC_DEACTIVATE_KEY_FF_4_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando DEACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt für DST ein falsches Tag besitzt. Dazu wird eine Kommandonachricht für DEACTIVATE KEY zum Deaktivieren eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.109.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_04, PN_04_08

2.109.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für DST)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.109.4 APDU-Kommandos

ID: CM-DEACTIVATE_KEY_FF_4_4						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	b6 LL [83 LL [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.109.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.109.6 Verifikationen

ID	Beschreibung
VF-DEACTIVATE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich auslesbar.

2.110 Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_4_5)

2.110.1 Informationen

ID	TC_DEACTIVATE_KEY_FF_4_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando DEACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-

	Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt für das Public-Key-Objekt ein falsches Tag besitzt. Dazu wird eine Kommandonachricht für DEACTIVATE KEY zum Deaktivieren eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.110.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_04, PN_04_08

2.110.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für das Public-Key-Objekt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.110.4 APDU-Kommandos

ID: CM-DEACTIVATE_KEY_FF_4_5

CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	a4 LL [83 LL [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.110.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.110.6 Verifikationen

ID	Beschreibung
VF-DEACTIVATE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich auslesbar.

2.111 Testfall: DEACTIVATE KEY (TC_DEACTIVATE_KEY_FF_4_6)

2.111.1 Informationen

ID	TC_DEACTIVATE_KEY_FF_4_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando DEACTIVATE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt für das Key-Pair-Objekt ein falsches Tag besitzt. Dazu wird eine Kommandonachricht für DEACTIVATE KEY zum Deaktivieren eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.111.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_04, PN_04_08

2.111.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für das Key-Pair-Objekt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.111.4 APDU-Kommandos

ID: CM-DEACTIVATE_KEY_FF_4_6						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	a4 LL [84 01 [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.111.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.111.6 Verifikationen

ID	Beschreibung
VF-DEACTIVATE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich auslesbar.

2.112 Testfall: DELETE FILE (TC_DELETE_FILE_GF_1)

2.112.1 Informationen

ID	TC_DELETE_FILE_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando DELETE FILE erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für DELETE FILE zum Löschen eines DFs/EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.112.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_18a

2.112.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_CURRENT_FILE-2	Das File ist ausgewählt
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.112.4 APDU-Kommandos

ID: CM-DELETE_FILE_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

2.112.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.112.6 Verifikationen

ID	Beschreibung
VF-DELETE_FILE-1	Das entsprechende File ist nicht mehr selektierbar.

2.113 Testfall: DELETE FILE (TC_DELETE_FILE_FF_1)

2.113.1 Informationen

ID	TC_DELETE_FILE_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando DELETE FILE nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im

	Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für DELETE FILE zum Löschen eines DFs/EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.113.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_18a

2.113.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-CURRENT_FILE-2	Das File ist ausgewählt
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.113.4 APDU-Kommandos

ID: CM-DELETE_FILE_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

2.113.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.113.6 Verifikationen

ID	Beschreibung
VF-DELETE_FILE-2	Das entsprechende File ist selektierbar.

2.114 Testfall: DELETE FILE (TC_DELETE_FILE_FF_2)

2.114.1 Informationen

ID	TC_DELETE_FILE_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando DELETE FILE nicht durchführen lässt, wenn das File vorher nicht selektiert wurde. Dazu wird eine Kommandonachricht für DELETE FILE zum Löschen eines DFs/EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.114.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_18a

2.114.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN- NO_CURRENT_FILE-1	Das File ist nicht ausgewählt
CN- INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.114.4 APDU-Kommandos

ID: CM-DELETE_FILE_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

2.114.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6986	Das Testsystem antwortet mit '69 86'.

2.114.6 Verifikationen

ID	Beschreibung
VF-DELETE_FILE-2	Das entsprechende File ist selektierbar.

2.115 Testfall: DELETE FILE (TC_DELETE_FILE_FF_3)

2.115.1 Informationen

ID	TC_DELETE_FILE_FF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando DELETE FILE nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Dazu wird eine Kommandonachricht für

	DELETE FILE zum Löschen eines DFs/EFs an das Sicherheitsmodul gesendet Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.115.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_18a

2.115.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-CURRENT_FILE-2	Das File ist ausgewählt

2.115.4 APDU-Kommandos

ID: CM-DELETE_FILE_FF_3						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

2.115.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.115.6 Verifikationen

ID	Beschreibung
VF-DELETE_FILE-2	Das entsprechende File ist selektierbar.

2.116 Testfall: DELETE KEY (TC_DELETE_KEY_GF_1_1)

2.116.1 Informationen

ID	TC_DELETE_KEY_GF_1_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando DELETE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Key-Objekt ist in diesem Fall ein Public-Key-Objekt für AT. Dazu wird eine Kommandonachricht für DELETE KEY zum Löschen eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.116.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_06, VI_02_03

2.116.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)

2.116.4 APDU-Kommandos

ID: CM-DELETE_KEY_GF_1_1						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	a4 LL [83 LL [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.116.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.116.6 Verifikationen

ID	Beschreibung
VF-DELETE_KEY-1	Das entsprechende Key-Objekt ist nicht selektierbar.

2.117 Testfall: DELETE KEY (TC_DELETE_KEY_GF_1_2)

2.117.1 Informationen

ID	TC_DELETE_KEY_GF_1_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando DELETE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Key-Objekt ist in diesem Fall ein Public-Key-Objekt für DST. Dazu wird eine Kommandonachricht für DELETE KEY zum Löschen eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.117.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_06, VI_02_03

2.117.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt

INCORRECT_PARA METERS-2	vorhandenes Datenobjekt für AT)

2.117.4 APDU-Kommandos

ID: CM-DELETE_KEY_GF_1_2						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	b6 LL [83 LL [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.117.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.117.6 Verifikationen

ID	Beschreibung
VF-DELETE_KEY-1	Das entsprechende Key-Objekt ist nicht selektierbar.

2.118 Testfall: DELETE KEY (TC_DELETE_KEY_GF_1_3)

2.118.1 Informationen

ID	TC_DELETE_KEY_GF_1_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando DELETE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Key-Objekt ist in diesem Fall ein Public-Key-Objekt für AT. Dazu wird eine Kommandonachricht für DELETE KEY zum Löschen eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche

	Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.118.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_06, VI_02_03

2.118.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)

2.118.4 APDU-Kommandos

ID: CM-DELETE_KEY_GF_1_3						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	a4 LL [84 01 [XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.118.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.118.6 Verifikationen

ID	Beschreibung
VF-DELETE_KEY-1	Das entsprechende Key-Objekt ist nicht selektierbar.

2.119 Testfall: DELETE KEY (TC_DELETE_KEY_GF_1_4)

2.119.1 Informationen

ID	TC_DELETE_KEY_GF_1_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando DELETE KEY erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Key-Objekt ist in diesem Fall ein Public-Key-Objekt für DST. Dazu wird eine Kommandonachricht für DELETE KEY zum Löschen eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.119.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_06, VI_02_03

2.119.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)

2.119.4 APDU-Kommandos

ID: CM-DELETE_KEY_GF_1_4						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	b6 LL [84 01 [XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.119.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.119.6 Verifikationen

ID	Beschreibung
VF-DELETE_KEY-1	Das entsprechende Key-Objekt ist nicht selektierbar.

2.120 Testfall: DELETE KEY (TC_DELETE_KEY_FF_1)

2.120.1 Informationen

ID	TC_DELETE_KEY_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando DELETE KEY nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für DELETE KEY zum Löschen eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.120.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_06, VI_02_03

2.120.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-	Key-Pair-Objekt kann gefunden werden

KEY_NOT_FOUND-2	
CN-SECURITY_STATU S_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)

2.120.4 APDU-Kommandos

ID: CM-DELETE_KEY_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	a4 LL [83 LL [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.120.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.120.6 Verifikationen

ID	Beschreibung
VF-DELETE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich selektierbar.

2.121 Testfall: DELETE KEY (TC_DELETE_KEY_FF_2_1)

2.121.1 Informationen

ID	TC_DELETE_KEY_FF_2_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando DELETE KEY nicht erfolgreich durchgeführt werden kann, wenn das Public-Key-Objekt für AT nicht gefunden wird. Dazu wird eine Kommandonachricht für DELETE KEY zum Löschen eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.121.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_06, VI_02_03

2.121.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- KEY_NOT_FOUND- 1	Public-Key-Objekt für AT kann nicht gefunden werden
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt

INCORRECT_PARA METERS-2	vorhandenes Datenobjekt für AT)

2.121.4 APDU-Kommandos

ID: CM-DELETE_KEY_FF_2_1						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	a4 LL [83 LL [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.121.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.121.6 Verifikationen

ID	Beschreibung
VF-DELETE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich selektierbar.

2.122 Testfall: DELETE KEY (TC_DELETE_KEY_FF_2_2)

2.122.1 Informationen

ID	TC_DELETE_KEY_FF_2_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando DELETE KEY nicht erfolgreich durchgeführt werden kann, wenn das Public-Key-Objekt für DST nicht gefunden wird. Dazu wird eine Kommandonachricht für DELETE KEY zum Löschen eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der

	Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.122.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_06, VI_02_03

2.122.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	Public-Key-Objekt für DST kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)

2.122.4 APDU-Kommandos

ID: CM-DELETE_KEY_FF_2_2						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	b6 LL [83 LL [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.122.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.122.6 Verifikationen

ID	Beschreibung
VF-DELETE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich selektierbar.

2.123 Testfall: DELETE KEY (TC_DELETE_KEY_FF_2_3)

2.123.1 Informationen

ID	TC_DELETE_KEY_FF_2_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando DELETE KEY nicht erfolgreich durchgeführt werden kann, wenn das Key-Pair-Objekt für AT nicht gefunden wird. Dazu wird eine Kommandonachricht für DELETE KEY zum Löschen eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.123.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_06, VI_02_03

2.123.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	Key-Pair-Objekt für AT kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)

2.123.4 APDU-Kommandos

ID: CM-DELETE_KEY_FF_2_3						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	a4 LL [84 01 [XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.123.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.123.6 Verifikationen

ID	Beschreibung
VF-DELETE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich selektierbar.

2.124 Testfall: DELETE KEY (TC_DELETE_KEY_FF_2_4)

2.124.1 Informationen

ID	TC_DELETE_KEY_FF_2_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando DELETE KEY nicht erfolgreich durchgeführt werden kann, wenn das Key-Pair-Objekt für DST nicht gefunden wird. Dazu wird eine Kommandonachricht für DELETE KEY zum Löschen eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.124.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_06, VI_02_03

2.124.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	Key-Pair-Objekt für DST kann nicht gefunden werden
CN-	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

INSTRUCTION_NO T_SUPPORTED-2	
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)

2.124.4 APDU-Kommandos

ID: CM-DELETE_KEY_FF_2_4						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	b6 LL [84 01 [XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.124.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.124.6 Verifikationen

ID	Beschreibung
VF-DELETE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich selektierbar.

2.125 Testfall: DELETE KEY (TC_DELETE_KEY_FF_3_1)

2.125.1 Informationen

ID	TC_DELETE_KEY_FF_3_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando DELETE KEY nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Nicht erfüllt bedeutet in diesem Testfall, dass eine notwendige Authentifizierung fehlt. Dazu wird eine Kommandonachricht für DELETE KEY zum Löschen eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.125.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_06, VI_02_03

2.125.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt (Authentifizierung nicht durchgeführt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden

CN- INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)

2.125.4 APDU-Kommandos

ID: CM-DELETE_KEY_FF_3_1						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	a4 LL [83 LL [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.125.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.125.6 Verifikationen

ID	Beschreibung
VF-DELETE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich selektierbar.

2.126 Testfall: DELETE KEY (TC_DELETE_KEY_FF_3_2)

2.126.1 Informationen

ID	TC_DELETE_KEY_FF_3_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando DELETE KEY nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Nicht erfüllt bedeutet in diesem Testfall, dass der notwendige PACE-Kanal nicht aufgebaut ist. Dazu wird eine Kommandonachricht für DELETE KEY zum Löschen eines Key-Objektes

	an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.126.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_06, VI_02_03

2.126.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt (PACE-Kanal nicht aufgebaut)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht doppelt vorhandenes Datenobjekt für AT)

2.126.4 APDU-Kommandos

ID: CM-DELETE_KEY_FF_3_2						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	a4 LL [83 LL [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.126.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.126.6 Verifikationen

ID	Beschreibung
VF-DELETE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich selektierbar.

2.127 Testfall: DELETE KEY (TC_DELETE_KEY_FF_4_1)

2.127.1 Informationen

ID	TC_DELETE_KEY_FF_4_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando DELETE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt für AT doppelt vorhanden ist. Dazu wird eine Kommandonachricht für DELETE KEY zum Löschen eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.127.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_06, VI_02_03

2.127.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Doppelt vorhandenes Datenobjekt für AT)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.127.4 APDU-Kommandos

ID: CM-DELETE_KEY_FF_4_1						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	a4 LL [83 LL [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.127.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.127.6 Verifikationen

ID	Beschreibung
VF-DELETE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich selektierbar.

2.128 Testfall: DELETE KEY (TC_DELETE_KEY_FF_4_2)

2.128.1 Informationen

ID	TC_DELETE_KEY_FF_4_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando DELETE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt für DST doppelt vorhanden ist. Dazu wird eine Kommandonachricht für DELETE KEY zum Löschen eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.128.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_06, VI_02_03

2.128.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Doppelt vorhandenes Datenobjekt für DST)

CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.128.4 APDU-Kommandos

ID: CM-DELETE_KEY_FF_4_2						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	b6 LL [83 LL [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.128.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.128.6 Verifikationen

ID	Beschreibung
VF-DELETE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich selektierbar.

2.129 Testfall: DELETE KEY (TC_DELETE_KEY_FF_4_3)

2.129.1 Informationen

ID	TC_DELETE_KEY_FF_4_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando DELETE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt für AT ein falsches Tag besitzt. Dazu wird eine Kommandonachricht für DELETE KEY zum Löschen eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.129.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_06, VI_02_03

2.129.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für AT)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

SECURITY_STATU S_NOT_SATISFIED- 2	

2.129.4 APDU-Kommandos

ID: CM-DELETE_KEY_FF_4_3						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	a4 LL [83 LL [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.129.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.129.6 Verifikationen

ID	Beschreibung
VF-DELETE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich selektierbar.

2.130 Testfall: DELETE KEY (TC_DELETE_KEY_FF_4_4)

2.130.1 Informationen

ID	TC_DELETE_KEY_FF_4_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando DELETE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt für DST ein falsches Tag besitzt. Dazu wird eine Kommandonachricht für DELETE KEY zum Löschen eines Key-Objektes

	an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.130.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_06, VI_02_03

2.130.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für DST)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.130.4 APDU-Kommandos

ID: CM-DELETE_KEY_FF_4_4						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	b6 LL [83 LL [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.130.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.130.6 Verifikationen

ID	Beschreibung
VF-DELETE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich selektierbar.

2.131 Testfall: DELETE KEY (TC_DELETE_KEY_FF_4_5)

2.131.1 Informationen

ID	TC_DELETE_KEY_FF_4_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando DELETE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt für das Public-Key-Objekt ein falsches Tag besitzt. Dazu wird eine Kommandonachricht für DELETE KEY zum Löschen eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.131.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_06, VI_02_03

2.131.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für das Public-Key-Objekt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.131.4 APDU-Kommandos

ID: CM-DELETE_KEY_FF_4_5						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	a4 LL [83 LL [XX...XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.131.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.131.6 Verifikationen

ID	Beschreibung
VF-DELETE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich selektierbar.

2.132 Testfall: DELETE KEY (TC_DELETE_KEY_FF_4_6)

2.132.1 Informationen

ID	TC_DELETE_KEY_FF_4_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando DELETE KEY nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Datenobjekt für das Key-Pair-Objekt ein falsches Tag besitzt. Dazu wird eine Kommandonachricht für DELETE KEY zum Löschen eines Key-Objektes an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.132.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.4.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_06, VI_02_03

2.132.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für das Key-Pair-Objekt)

CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (Authentifizierung durchgeführt)

2.132.4 APDU-Kommandos

ID: CM-DELETE_KEY_FF_4_6						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	a4 LL [84 01 [XX]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

2.132.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.132.6 Verifikationen

ID	Beschreibung
VF-DELETE_KEY-2	Das entsprechende Key-Objekt ist erfolgreich selektierbar.

2.133 Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_GF_1_1)

2.133.1 Informationen

ID	TC_EXTERNAL_AUTHENTICATE_GF_1_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando EXTERNAL AUTHENTICATE erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Die Durchführung erfolgt für ECDSA mit SHSA256. Dazu wird eine Kommandonachricht für EXTERNAL AUTHENTICATE zur Authentisierung eines GW-Administrators an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.133.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.133.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-NO_ERROR-1	Es muss das Kommando GET CHALLENGE (Kommando-Variante mit Sicherheitsmodul-interner Verfügbarkeit der generierten Challenge) abgesetzt worden sein
CN-NO_ERROR-2	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Public-Key-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

CN- NO_KEY_REFEREN CE-2	Key-Objekt ist ausgewählt
CN- UNSUPPORTED_FU NCTION-2	Schlüssel für AT unterstützt Algorithmus
CN-KEY_INVALID- 2	Key-Daten sind vorhanden (ECDSA mit SHA256)
CN- OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-NO_RANDOM-2	Zufallszahl ist vorhanden
CN- WRONG_RANDOM _LENGTH-2	Zufallszahlen haben die richtige Länge
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.133.4 APDU-Kommandos

ID: CM-EXTERNAL_AUTHENTICATE_GF_1_1						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

2.133.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.133.6 Verifikationen

ID	Beschreibung
VF-EXTERNAL_AUTHENTICATE-1	Der Sicherheitszustand AUTH ist gesetzt.

2.134 Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_GF_1_2)

2.134.1 Informationen

ID	TC_EXTERNAL_AUTHENTICATE_GF_1_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando EXTERNAL AUTHENTICATE erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Die Durchführung erfolgt für ECDSA mit SHA384. Dazu wird eine Kommandonachricht für EXTERNAL AUTHENTICATE zur Authentisierung eines GW-Administrators an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.134.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.134.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-NO_ERROR-1	Es muss das Kommando GET CHALLENGE (Kommando-Variante mit Sicherheitsmodul-interner Verfügbarkeit der generierten Challenge) abgesetzt worden sein
CN-NO_ERROR-2	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Public-Key-Objektes) abgesetzt worden sein.

CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel für AT unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden (ECDSA mit SHA256)
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-NO_RANDOM-2	Zufallszahl ist vorhanden
CN-WRONG_RANDOM_LENGTH-2	Zufallszahlen haben die richtige Länge
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.134.4 APDU-Kommandos

ID: CM-EXTERNAL_AUTHENTICATE_GF_1_2						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

2.134.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.134.6 Verifikationen

ID	Beschreibung
VF-EXTERNAL_AUTHENTICATE-1	Der Sicherheitszustand AUTH ist gesetzt.

2.135 Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_GF_1_3)

2.135.1 Informationen

ID	TC_EXTERNAL_AUTHENTICATE_GF_1_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando EXTERNAL AUTHENTICATE erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Die Durchführung erfolgt für ECDSA mit SHA512. Dazu wird eine Kommandonachricht für EXTERNAL AUTHENTICATE zur Authentisierung eines GW-Administrators an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.135.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.135.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-NO_ERROR-1	Es muss das Kommando GET CHALLENGE (Kommando-Variante mit

	Sicherheitsmodul-interner Verfügbarkeit der generierten Challenge) abgesetzt worden sein
CN-NO_ERROR-2	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Public-Key-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel für AT unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden (ECDSA mit SHA256)
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-NO_RANDOM-2	Zufallszahl ist vorhanden
CN-WRONG_RANDOM_LENGTH-2	Zufallszahlen haben die richtige Länge
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.135.4 APDU-Kommandos

ID: CM-EXTERNAL_AUTHENTICATE_GF_1_3						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

2.135.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.135.6 Verifikationen

ID	Beschreibung
VF-EXTERNAL_AUTHENTICATE-1	Der Sicherheitszustand AUTH ist gesetzt.

2.136 Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_GF_2_1)

2.136.1 Informationen

ID	TC_EXTERNAL_AUTHENTICATE_GF_2_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando EXTERNAL AUTHENTICATE mit einem manipulierten Kryptogramm erfolgreich mit der entsprechenden Fehlermeldung abgebrochen wird. Die Durchführung erfolgt für ECDSA mit SHA256. Dazu wird eine Kommandonachricht für EXTERNAL AUTHENTICATE zur Authentisierung eines GW-Administrators an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.136.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.136.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-AUTHENTICATION_ERROR-1	Es muss das Kommando GET CHALLENGE (Kommando-Variante mit Sicherheitsmodul-interner Verfügbarkeit der generierten Challenge) abgesetzt worden sein
CN-AUTHENTICATION_ERROR-2	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Public-Key-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel für AT unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden (ECDSA mit SHA256)
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-NO_RANDOM-2	Zufallszahl ist vorhanden
CN-WRONG_RANDOM_LENGTH-2	Zufallszahlen haben die richtige Länge
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.136.4 APDU-Kommandos

ID: CM-EXTERNAL_AUTHENTICATE_GF_2_1

CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

2.136.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6300	Das Testsystem antwortet mit '63 00'.

2.136.6 Verifikationen

ID	Beschreibung
VF-EXTERNAL_AUTHENTICATE-1	Der Sicherheitszustand AUTH ist gesetzt.

2.137 Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_GF_2_2)

2.137.1 Informationen

ID	TC_EXTERNAL_AUTHENTICATE_GF_2_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando EXTERNAL AUTHENTICATE mit einem manipulierten Kryptogramm erfolgreich mit der entsprechenden Fehlermeldung abgebrochen wird. Die Durchführung erfolgt für ECDSA mit SHA384. Dazu wird eine Kommandonachricht für EXTERNAL AUTHENTICATE zur Authentisierung eines GW-Administrators an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.137.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.137.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-AUTHENTICATION_ERROR-1	Es muss das Kommando GET CHALLENGE (Kommando-Variante mit Sicherheitsmodul-interner Verfügbarkeit der generierten Challenge) abgesetzt worden sein
CN-AUTHENTICATION_ERROR-2	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Public-Key-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel für AT unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden (ECDSA mit SHA256)
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-NO_RANDOM-2	Zufallszahl ist vorhanden
CN-WRONG_RANDOM_LENGTH-2	Zufallszahlen haben die richtige Länge
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.137.4 APDU-Kommandos

ID: CM-EXTERNAL_AUTHENTICATE_GF_2_2						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

2.137.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6300	Das Testsystem antwortet mit '63 00'.

2.137.6 Verifikationen

ID	Beschreibung
VF-EXTERNAL_AUTHENTICATE-1	Der Sicherheitszustand AUTH ist gesetzt.

2.138 Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_GF_2_3)

2.138.1 Informationen

ID	TC_EXTERNAL_AUTHENTICATE_GF_2_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando EXTERNAL AUTHENTICATE mit einem manipulierten Kryptogramm erfolgreich mit der entsprechenden Fehlermeldung abgebrochen wird. Die Durchführung erfolgt für ECDSA mit SHA512. Dazu wird eine Kommandonachricht für EXTERNAL AUTHENTICATE zur Authentisierung eines GW-Administrators an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.138.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.138.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-AUTHENTICATION_ERROR-1	Es muss das Kommando GET CHALLENGE (Kommando-Variante mit Sicherheitsmodul-interner Verfügbarkeit der generierten Challenge) abgesetzt worden sein
CN-AUTHENTICATION_ERROR-2	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Public-Key-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel für AT unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden (ECDSA mit SHA256)
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-NO_RANDOM-2	Zufallszahl ist vorhanden
CN-WRONG_RANDOM_LENGTH-2	Zufallszahlen haben die richtige Länge

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.138.4 APDU-Kommandos

ID: CM-EXTERNAL_AUTHENTICATE_GF_2_3						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

2.138.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6300	Das Testsystem antwortet mit '63 00'.

2.138.6 Verifikationen

ID	Beschreibung
VF-EXTERNAL_AUTHENTICATE-1	Der Sicherheitszustand AUTH ist gesetzt.

2.139 Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_1)

2.139.1 Informationen

ID	TC_EXTERNAL_AUTHENTICATE_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando EXTERNAL AUTHENTICATE nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für EXTERNAL AUTHENTICATE zur Authentisierung eines GW-Administrators an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des

	Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.139.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.139.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-INSTRUCTION_NO T_SUPPORTED-1	Es muss das Kommando GET CHALLENGE (Kommando-Variante mit Sicherheitsmodul-interner Verfügbarkeit der generierten Challenge) abgesetzt worden sein
CN-INSTRUCTION_NO T_SUPPORTED-2	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Public-Key-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NO T_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel für AT unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden (ECDSA mit SHA256)
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

CN-NO_RANDOM-2	Zufallszahl ist vorhanden
CN-WRONG_RANDOM_LENGTH-2	Zufallszahlen haben die richtige Länge
CN-SECURITY_STATU S_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.139.4 APDU-Kommandos

ID: CM-EXTERNAL_AUTHENTICATE_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

2.139.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.139.6 Verifikationen

ID	Beschreibung
VF-EXTERNAL_AUTHENTICATE-2	Der Sicherheitszustand AUTH ist nicht gesetzt.

2.140 Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_2)

2.140.1 Informationen

ID	TC_EXTERNAL_AUTHENTICATE_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando EXTERNAL

	AUTHENTICATE nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt nicht ausgewählt ist. Dazu wird eine Kommandonachricht für EXTERNAL AUTHENTICATE zur Authentisierung eines GW-Administrators an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.140.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.140.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-NO_KEY_REFERENC CE-1	Es muss das Kommando GET CHALLENGE (Kommando-Variante mit Sicherheitsmodul-interner Verfügbarkeit der generierten Challenge) abgesetzt worden sein
CN-NO_KEY_REFERENC CE-2	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Public-Key-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-NO_KEY_REFERENC CE-1	Key-Objekt ist nicht ausgewählt
CN-INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-UNSUPPORTED_FU NCTION-2	Schlüssel für AT unterstützt Algorithmus
CN-KEY_INVALID- 2	Key-Daten sind vorhanden (ECDSA mit SHA256)

CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-NO_RANDOM-2	Zufallszahl ist vorhanden
CN-WRONG_RANDOM_LENGTH-2	Zufallszahlen haben die richtige Länge
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.140.4 APDU-Kommandos

ID: CM-EXTERNAL_AUTHENTICATE_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

2.140.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6985	Das Testsystem antwortet mit '69 85'.

2.140.6 Verifikationen

ID	Beschreibung
VF-EXTERNAL_AUTHENTICATE-2	Der Sicherheitszustand AUTH ist nicht gesetzt.

2.141 Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_3_1)

2.141.1 Informationen

ID	TC_EXTERNAL_AUTHENTICATE_FF_3_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando EXTERNAL AUTHENTICATE nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt mit einem Schlüssel für AT. Dazu wird eine Kommandonachricht für EXTERNAL AUTHENTICATE zur Authentisierung eines GW-Administrators an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.141.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.141.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-UNSUPPORTED_FUNCTION-1	Es muss das Kommando GET CHALLENGE (Kommando-Variante mit Sicherheitsmodul-interner Verfügbarkeit der generierten Challenge) abgesetzt worden sein
CN-UNSUPPORTED_FUNCTION-2	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Public-Key-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel für AT unterstützt Algorithmus nicht

CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_INVALID-2	Key-Daten sind vorhanden (ECDSA mit SHA256)
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-NO_RANDOM-2	Zufallszahl ist vorhanden
CN-WRONG_RANDOM_LENGTH-2	Zufallszahlen haben die richtige Länge
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.141.4 APDU-Kommandos

ID: CM-EXTERNAL_AUTHENTICATE_FF_3_1						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

2.141.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.141.6 Verifikationen

ID	Beschreibung
VF-EXTERNAL_AUTHENTICATE-2	Der Sicherheitszustand AUTH ist nicht gesetzt.

2.142 Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_3_2)

2.142.1 Informationen

ID	TC_EXTERNAL_AUTHENTICATE_FF_3_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando EXTERNAL AUTHENTICATE nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt mit einem Schlüssel für DST. Dazu wird eine Kommandonachricht für EXTERNAL AUTHENTICATE zur Authentisierung eines GW-Administrators an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.142.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.142.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-UNSUPPORTED_FUNCTION-1	Es muss das Kommando GET CHALLENGE (Kommando-Variante mit Sicherheitsmodul-interner Verfügbarkeit der generierten Challenge) abgesetzt worden sein
CN-UNSUPPORTED_FUNCTION-2	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Public-Key-Objektes) abgesetzt worden sein.

CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel für DST unterstützt Algorithmus nicht
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_INVALID-2	Key-Daten sind vorhanden (ECDSA mit SHA256)
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-NO_RANDOM-2	Zufallszahl ist vorhanden
CN-WRONG_RANDOM_LENGTH-2	Zufallszahlen haben die richtige Länge
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.142.4 APDU-Kommandos

ID: CM-EXTERNAL_AUTHENTICATE_FF_3_2						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

2.142.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.142.6 Verifikationen

ID	Beschreibung
VF-EXTERNAL_AUTHENTICATE-2	Der Sicherheitszustand AUTH ist nicht gesetzt.

2.143 Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_4_1)

2.143.1 Informationen

ID	TC_EXTERNAL_AUTHENTICATE_FF_4_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando EXTERNAL AUTHENTICATE nicht erfolgreich durchgeführt werden kann, wenn die Key-Daten nicht vorhanden sind. Die Durchführung erfolgt für ECDSA mit SHA256. Dazu wird eine Kommandonachricht für EXTERNAL AUTHENTICATE zur Authentisierung eines GW-Administrators an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.143.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.143.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-KEY_INVALID-	Es muss das Kommando GET CHALLENGE (Kommando-Variante mit

1	Sicherheitsmodul-interner Verfügbarkeit der generierten Challenge) abgesetzt worden sein
CN-KEY_INVALID-2	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Public-Key-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_INVALID-1	Key-Daten sind nicht vorhanden (ECDSA mit SHA256)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel für AT unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-NO_RANDOM-2	Zufallszahl ist vorhanden
CN-WRONG_RANDOM_LENGTH-2	Zufallszahlen haben die richtige Länge
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.143.4 APDU-Kommandos

ID: CM-EXTERNAL_AUTHENTICATE_FF_4_1						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

2.143.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6400	Das Testsystem antwortet mit '64 00'.

2.143.6 Verifikationen

ID	Beschreibung
VF-EXTERNAL_AUTHENTICATE-2	Der Sicherheitszustand AUTH ist nicht gesetzt.

2.144 Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_4_2)

2.144.1 Informationen

ID	TC_EXTERNAL_AUTHENTICATE_FF_4_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando EXTERNAL AUTHENTICATE nicht erfolgreich durchgeführt werden kann, wenn die Key-Daten nicht vorhanden sind. Die Durchführung erfolgt für ECDSA mit SHA384. Dazu wird eine Kommandonachricht für EXTERNAL AUTHENTICATE zur Authentisierung eines GW-Administrators an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.144.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.144.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-KEY_INVALID-1	Es muss das Kommando GET CHALLENGE (Kommando-Variante mit Sicherheitsmodul-interner Verfügbarkeit der generierten Challenge) abgesetzt worden sein
CN-KEY_INVALID-2	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Public-Key-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_INVALID-1	Key-Daten sind nicht vorhanden (ECDSA mit SHA384)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel für AT unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-NO_RANDOM-2	Zufallszahl ist vorhanden
CN-WRONG_RANDOM_LENGTH-2	Zufallszahlen haben die richtige Länge
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.144.4 APDU-Kommandos

ID: CM-EXTERNAL_AUTHENTICATE_FF_4_2

CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

2.144.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6400	Das Testsystem antwortet mit '64 00'.

2.144.6 Verifikationen

ID	Beschreibung
VF-EXTERNAL_AUTHENTICATE-2	Der Sicherheitszustand AUTH ist nicht gesetzt.

2.145 Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_4_3)

2.145.1 Informationen

ID	TC_EXTERNAL_AUTHENTICATE_FF_4_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando EXTERNAL AUTHENTICATE nicht erfolgreich durchgeführt werden kann, wenn die Key-Daten nicht vorhanden sind. Die Durchführung erfolgt für ECDSA mit SHA512. Dazu wird eine Kommandonachricht für EXTERNAL AUTHENTICATE zur Authentisierung eines GW-Administrators an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.145.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.145.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-KEY_INVALID-1	Es muss das Kommando GET CHALLENGE (Kommando-Variante mit Sicherheitsmodul-interner Verfügbarkeit der generierten Challenge) abgesetzt worden sein
CN-KEY_INVALID-2	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Public-Key-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_INVALID-1	Key-Daten sind nicht vorhanden (ECDSA mit SHA512)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel für AT unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-NO_RANDOM-2	Zufallszahl ist vorhanden
CN-WRONG_RANDOM_LENGTH-2	Zufallszahlen haben die richtige Länge
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.145.4 APDU-Kommandos

ID: CM-EXTERNAL_AUTHENTICATE_FF_4_3						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

2.145.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6400	Das Testsystem antwortet mit '64 00'.

2.145.6 Verifikationen

ID	Beschreibung
VF-EXTERNAL_AUTHENTICATE-2	Der Sicherheitszustand AUTH ist nicht gesetzt.

2.146 Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_5)

2.146.1 Informationen

ID	TC_EXTERNAL_AUTHENTICATE_FF_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando EXTERNAL AUTHENTICATE nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Dazu wird eine Kommandonachricht für EXTERNAL AUTHENTICATE zur Authentisierung eines GW-Administrators an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.146.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.146.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-OBJECT_DEACTIVATED-1	Es muss das Kommando GET CHALLENGE (Kommando-Variante mit Sicherheitsmodul-interner Verfügbarkeit der generierten Challenge) abgesetzt worden sein
CN-OBJECT_DEACTIVATED-2	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Public-Key-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_DEACTIVATED-1	Key-Objekt befindet sich im Zustand "operational state - deactivated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel für AT unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden (ECDSA mit SHA256)
CN-NO_RANDOM-2	Zufallszahl ist vorhanden
CN-WRONG_RANDOM_LENGTH-2	Zufallszahlen haben die richtige Länge

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.146.4 APDU-Kommandos

ID: CM-EXTERNAL_AUTHENTICATE_FF_5						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

2.146.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.146.6 Verifikationen

ID	Beschreibung
VF-EXTERNAL_AUTHENTICATE-2	Der Sicherheitszustand AUTH ist nicht gesetzt.

2.147 Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_6_1)

2.147.1 Informationen

ID	TC_EXTERNAL_AUTHENTICATE_FF_6_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando EXTERNAL AUTHENTICATE nicht erfolgreich durchgeführt werden kann, wenn keine Zufallszahlen vorhanden sind. Die Durchführung erfolgt für ECDSA mit SHA256. Dazu wird eine Kommandonachricht für EXTERNAL AUTHENTICATE zur Authentisierung eines GW-Administrators an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche

	Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.147.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.147.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-NO_RANDOM-1	Es muss das Kommando GET CHALLENGE (Kommando-Variante mit Sicherheitsmodul-interner Verfügbarkeit der generierten Challenge) abgesetzt worden sein
CN-NO_RANDOM-2	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Public-Key-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-NO_RANDOM-1	Zufallszahl ist nicht vorhanden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel für AT unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden (ECDSA mit SHA256)
CN-OBJECT_DEACTIVATED	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

ATED-2	
CN-WRONG_RANDOM_LENGTH-2	Zufallszahlen haben die richtige Länge
CN-SECURITY_STATU S_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.147.4 APDU-Kommandos

ID: CM-EXTERNAL_AUTHENTICATE_FF_6_1						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

2.147.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6985	Das Testsystem antwortet mit '69 85'.

2.147.6 Verifikationen

ID	Beschreibung
VF-EXTERNAL_AUTHENTICATE-2	Der Sicherheitszustand AUTH ist nicht gesetzt.

2.148 Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_6_2)

2.148.1 Informationen

ID	TC_EXTERNAL_AUTHENTICATE_FF_6_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando EXTERNAL

	AUTHENTICATE nicht erfolgreich durchgeführt werden kann, wenn keine Zufallszahlen vorhanden sind. Die Durchführung erfolgt für ECDSA mit SHA384. Dazu wird eine Kommandonachricht für EXTERNAL AUTHENTICATE zur Authentisierung eines GW-Administrators an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.148.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.148.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-NO_RANDOM-1	Es muss das Kommando GET CHALLENGE (Kommando-Variante mit Sicherheitsmodul-interner Verfügbarkeit der generierten Challenge) abgesetzt worden sein
CN-NO_RANDOM-2	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Public-Key-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-NO_RANDOM-1	Zufallszahl ist nicht vorhanden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel für AT unterstützt Algorithmus

CN-KEY_INVALID-2	Key-Daten sind vorhanden (ECDSA mit SHA256)
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-WRONG_RANDOM_LENGTH-2	Zufallszahlen haben die richtige Länge
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.148.4 APDU-Kommandos

ID: CM-EXTERNAL_AUTHENTICATE_FF_6_2						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

2.148.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6985	Das Testsystem antwortet mit '69 85'.

2.148.6 Verifikationen

ID	Beschreibung
VF-EXTERNAL_AUTHENTICATE-2	Der Sicherheitszustand AUTH ist nicht gesetzt.

2.149 Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_6_3)

2.149.1 Informationen

ID	TC_EXTERNAL_AUTHENTICATE_FF_6_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando EXTERNAL AUTHENTICATE nicht erfolgreich durchgeführt werden kann, wenn keine Zufallszahlen vorhanden sind. Die Durchführung erfolgt für ECDSA mit SHA512. Dazu wird eine Kommandonachricht für EXTERNAL AUTHENTICATE zur Authentisierung eines GW-Administrators an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.149.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.149.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-NO_RANDOM-1	Es muss das Kommando GET CHALLENGE (Kommando-Variante mit Sicherheitsmodul-interner Verfügbarkeit der generierten Challenge) abgesetzt worden sein
CN-NO_RANDOM-2	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Public-Key-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-NO_RANDOM-1	Zufallszahl ist nicht vorhanden
CN-	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

INSTRUCTION_NO T_SUPPORTED-2	
CN- NO_KEY_REFEREN CE-2	Key-Objekt ist ausgewählt
CN- UNSUPPORTED_FU NCTION-2	Schlüssel für AT unterstützt Algorithmus
CN-KEY_INVALID- 2	Key-Daten sind vorhanden (ECDSA mit SHA256)
CN- OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN- WRONG_RANDOM _LENGTH-2	Zufallszahlen haben die richtige Länge
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.149.4 APDU-Kommandos

ID: CM-EXTERNAL_AUTHENTICATE_FF_6_3						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

2.149.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6985	Das Testsystem antwortet mit '69 85'.

2.149.6 Verifikationen

ID	Beschreibung
VF-EXTERNAL_AUTHENTICATE-2	Der Sicherheitszustand AUTH ist nicht gesetzt.

2.150 Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_7_1)

2.150.1 Informationen

ID	TC_EXTERNAL_AUTHENTICATE_FF_7_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando EXTERNAL AUTHENTICATE nicht erfolgreich durchgeführt werden kann, wenn die Zufallszahlen die falsche Länge haben. Die Durchführung erfolgt für ECDSA mit SHA256. Dazu wird eine Kommandonachricht für EXTERNAL AUTHENTICATE zur Authentisierung eines GW-Administrators an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.150.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.150.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-WRONG_RANDOM_LENGTH-1	Es muss das Kommando GET CHALLENGE (Kommando-Variante mit Sicherheitsmodul-interner Verfügbarkeit der generierten Challenge) abgesetzt worden sein
CN-WRONG_RANDOM_LENGTH-2	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Public-Key-Objektes) abgesetzt worden sein.

CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-WRONG_RANDOM_LENGTH-1	Zufallszahlen haben nicht die richtige Länge
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel für AT unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden (ECDSA mit SHA256)
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-NO_RANDOM-2	Zufallszahl ist vorhanden
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.150.4 APDU-Kommandos

ID: CM-EXTERNAL_AUTHENTICATE_FF_7_1						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

2.150.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6985	Das Testsystem antwortet mit '69 85'.

2.150.6 Verifikationen

ID	Beschreibung
VF-EXTERNAL_AUTHENTICATE-2	Der Sicherheitszustand AUTH ist nicht gesetzt.

2.151 Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_7_2)

2.151.1 Informationen

ID	TC_EXTERNAL_AUTHENTICATE_FF_7_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando EXTERNAL AUTHENTICATE nicht erfolgreich durchgeführt werden kann, wenn die Zufallszahlen die falsche Länge haben. Die Durchführung erfolgt für ECDSA mit SHA384. Dazu wird eine Kommandonachricht für EXTERNAL AUTHENTICATE zur Authentisierung eines GW-Administrators an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.151.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.151.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-	Es muss das Kommando GET CHALLENGE (Kommando-Variante mit

WRONG_RANDOM_LENGTH-1	Sicherheitsmodul-interner Verfügbarkeit der generierten Challenge) abgesetzt worden sein
CN-WRONG_RANDOM_LENGTH-2	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Public-Key-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-WRONG_RANDOM_LENGTH-1	Zufallszahlen haben nicht die richtige Länge
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel für AT unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden (ECDSA mit SHA256)
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-NO_RANDOM-2	Zufallszahl ist vorhanden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.151.4 APDU-Kommandos

ID: CM-EXTERNAL_AUTHENTICATE_FF_7_2						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

2.151.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6985	Das Testsystem antwortet mit '69 85'.

2.151.6 Verifikationen

ID	Beschreibung
VF-EXTERNAL_AUTHENTICATE-2	Der Sicherheitszustand AUTH ist nicht gesetzt.

2.152 Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_7_3)

2.152.1 Informationen

ID	TC_EXTERNAL_AUTHENTICATE_FF_7_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando EXTERNAL AUTHENTICATE nicht erfolgreich durchgeführt werden kann, wenn die Zufallszahlen die falsche Länge haben. Die Durchführung erfolgt für ECDSA mit SHA512. Dazu wird eine Kommandonachricht für EXTERNAL AUTHENTICATE zur Authentisierung eines GW-Administrators an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.152.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.152.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-WRONG_RANDOM_LENGTH-1	Es muss das Kommando GET CHALLENGE (Kommando-Variante mit Sicherheitsmodul-interner Verfügbarkeit der generierten Challenge) abgesetzt worden sein
CN-WRONG_RANDOM_LENGTH-2	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Public-Key-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-WRONG_RANDOM_LENGTH-1	Zufallszahlen haben nicht die richtige Länge
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel für AT unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden (ECDSA mit SHA256)
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-NO_RANDOM-2	Zufallszahl ist vorhanden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.152.4 APDU-Kommandos

ID: CM-EXTERNAL_AUTHENTICATE_FF_7_3

CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

2.152.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6985	Das Testsystem antwortet mit '69 85'.

2.152.6 Verifikationen

ID	Beschreibung
VF-EXTERNAL_AUTHENTICATE-2	Der Sicherheitszustand AUTH ist nicht gesetzt.

2.153 Testfall: EXTERNAL AUTHENTICATE (TC_EXTERNAL_AUTHENTICATE_FF_8)

2.153.1 Informationen

ID	TC_EXTERNAL_AUTHENTICATE_FF_8
Beschreibung	Dieser Test verifiziert, dass ein Kommando EXTERNAL AUTHENTICATE nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Dazu wird eine Kommandonachricht für EXTERNAL AUTHENTICATE zur Authentisierung eines GW-Administrators an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.153.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.153.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SECURITY_STATU S_NOT_SATISFIED- 1	Es muss das Kommando GET CHALLENGE (Kommando-Variante mit Sicherheitsmodul-interner Verfügbarkeit der generierten Challenge) abgesetzt worden sein
CN-SECURITY_STATU S_NOT_SATISFIED- 2	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Public-Key-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATU S_NOT_SATISFIED- 1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFEREN CE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FU NCTION-2	Schlüssel für AT unterstützt Algorithmus
CN-KEY_INVALID- 2	Key-Daten sind vorhanden (ECDSA mit SHA256)
CN-OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-NO_RANDOM-2	Zufallszahl ist vorhanden
CN-WRONG_RANDOM _LENGTH-2	Zufallszahlen haben die richtige Länge

2.153.4 APDU-Kommandos

ID: CM-EXTERNAL_AUTHENTICATE_FF_8						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

2.153.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.153.6 Verifikationen

ID	Beschreibung
VF-EXTERNAL_AUTHENTICATE-2	Der Sicherheitszustand AUTH ist nicht gesetzt.

2.154 Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_GF_1_1)

2.154.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_ECKA_GF_1_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels ECKA erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Die Durchführung erfolgt für ECKA-DH mit implizit bekannter elliptischer Kurve. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels ECKA zur Realisierung von Kernroutinen für das Key-Agreement an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.154.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06

2.154.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-NO_ERROR-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETER	Parameter im Kommando-Datenfeld sind korrekt (nicht fehlendes 7c-Tag)

METERS-2	

2.154.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_ECKA_GF_1_1						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

2.154.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.154.6 Verifikationen

n/a

2.155 Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_GF_1_2)

2.155.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_ECKA_GF_1_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels ECKA erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Die Durchführung

	erfolgt für ECKA-DH ohne implizit bekannter elliptischer Kurve. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels ECKA zur Realisierung von Kernroutinen für das Key-Agreement an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.155.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06

2.155.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-NO_ERROR-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-UNSUPPORTED_FUNCTION	Schlüssel unterstützt Algorithmus

NCTION-2	
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht fehlendes 7c-Tag)

2.155.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_ECKA_GF_1_2						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

2.155.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.155.6 Verifikationen

n/a

2.156 Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_GF_2_1)

2.156.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_ECKA_GF_2_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels ECKA erfolgreich durchgeführt werden kann und das Protokoll fehlschlägt. Die Durchführung erfolgt für ECKA-DH mit vorhandener, aber unerlaubter OID. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels ECKA zur Realisierung von Kernroutinen für das Key-Agreement an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.156.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06

2.156.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PROTOCOL_ERROR-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCED	Key-Objekt ist ausgewählt

CE-2	
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATU S_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-UNSUPPORTED_FU NCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht fehlendes 7c-Tag)

2.156.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_ECKA_GF_2_1						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

2.156.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6300	Das Testsystem antwortet mit '63 00'.

2.156.6 Verifikationen

n/a

2.157 Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_GF_2_2)

2.157.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_ECKA_GF_2_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels ECKA erfolgreich durchgeführt werden kann und das Protokoll fehlschlägt. Die Durchführung erfolgt für ECKA-DH mit manipuliertem übergebenem Schlüssel. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels ECKA zur Realisierung von Kernroutinen für das Key-Agreement an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.157.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06

2.157.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN- PROTOCOL_ERRO	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.

R-1	
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht fehlendes 7c-Tag)

2.157.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_ECKA_GF_2_2						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

2.157.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6300	Das Testsystem antwortet mit '63 00'.

2.157.6 Verifikationen

n/a

2.158 Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_FF_1)

2.158.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_ECKA_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels ECKA nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels ECKA zur Realisierung von Kernroutinen für das Key-Agreement an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.158.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06

2.158.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-INSTRUCTION_NOT_SUPPORTED-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht fehlendes 7c-Tag)

2.158.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_ECKA_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

2.158.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.158.6 Verifikationen

ID	Beschreibung
VF-GENERAL_AUTHENTICATE_ECKA_DH-1	Der ausgehandelte Schlüssel ist in nachfolgenden Krypto-Operationen (z. B. Test der Zugriffsrechte eines neuen File) nicht verwendbar.

2.159 Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_FF_2)

2.159.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_ECKA_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL

	AUTHENTICATE mittels ECKA nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt nicht ausgewählt ist. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels ECKA zur Realisierung von Kernroutinen für das Key-Agreement an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.159.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06

2.159.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-NO_KEY_REFERENC-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-NO_KEY_REFERENC-1	Key-Objekt ist nicht ausgewählt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)

CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht fehlendes 7c-Tag)

2.159.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_ECKA_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

2.159.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6985	Das Testsystem antwortet mit '69 85'.

2.159.6 Verifikationen

ID	Beschreibung
VF-	Der ausgehandelte Schlüssel ist in

GENERAL_AUTHENTICATE_ECKA_DH-1	nachfolgenden Krypto-Operationen (z. B. Test der Zugriffsrechte eines neuen File) nicht verwendbar.

2.160 Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_FF_3)

2.160.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_ECKA_FF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels ECKA nicht erfolgreich durchgeführt werden kann, wenn das KEY-Objekt nicht gefunden wird. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels ECKA zur Realisierung von Kernroutinen für das Key-Agreement an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.160.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06

2.160.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-KEY_NOT_FOUND-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-	KEY-Objekt kann nicht gefunden werden

1	
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht fehlendes 7c-Tag)

2.160.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_ECKA_FF_3						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit

SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

2.160.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.160.6 Verifikationen

ID	Beschreibung
VF- GENERAL_AUTHENTICATE_ECKA_DH-1	Der ausgehandelte Schlüssel ist in nachfolgenden Krypto-Operationen (z. B. Test der Zugriffsrechte eines neuen File) nicht verwendbar.

2.161 Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_FF_4)

2.161.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_ECKA_FF_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels ECKA nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Nicht erfüllt bedeutet in diesem Testfall, dass der notwendige PACE-Kanal nicht aufgebaut ist. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels ECKA zur Realisierung von Kernroutinen für das Key-Agreement an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.161.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06

2.161.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SECURITY_STATU S_NOT_SATISFIED- 1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATU S_NOT_SATISFIED- 1	Zugriffsregel ist nicht erfüllt (PACE-Kanal nicht aufgebaut)
CN-INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFEREN CE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND- 2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FU NCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALIDID- 2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht fehlendes 7c-Tag)

2.161.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_ECKA_FF_4						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

2.161.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.161.6 Verifikationen

ID	Beschreibung
VF-GENERAL_AUTHENTICATE_ECKA_DH-1	Der ausgehandelte Schlüssel ist in nachfolgenden Krypto-Operationen (z. B. Test der Zugriffsrechte eines neuen File) nicht verwendbar.

2.162 Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_FF_5)

2.162.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_ECKA_FF_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL

	AUTHENTICATE mittels ECKA nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels ECKA zur Realisierung von Kernroutinen für das Key-Agreement an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.162.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06

2.162.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-UNSUPPORTED_FUNCTION-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)

SECURITY_STATU S_NOT_SATISFIED- 2	
CN-KEY_INVALID- 2	Key-Daten sind vorhanden
CN- OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht fehlendes 7c-Tag)

2.162.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_ECKA_FF_5						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

2.162.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.162.6 Verifikationen

ID	Beschreibung
VF-	Der ausgehandelte Schlüssel ist in

GENERAL_AUTHENTICATE_ECKA_DH-1	nachfolgenden Krypto-Operationen (z. B. Test der Zugriffsrechte eines neuen File) nicht verwendbar.

2.163 Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_FF_6)

2.163.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_ECKA_FF_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels ECKA nicht erfolgreich durchgeführt werden kann, wenn die Key-Daten nicht vorhanden sind. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels ECKA zur Realisierung von Kernroutinen für das Key-Agreement an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.163.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06

2.163.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-KEY_INVALID-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_INVALID-1	Key-Daten sind nicht vorhanden

CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht fehlendes 7c-Tag)

2.163.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_ECKA_FF_6						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

2.163.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6400	Das Testsystem antwortet mit '64 00'.

2.163.6 Verifikationen

ID	Beschreibung
VF- GENERAL_AUTHENTICATE_ECKA_DH-1	Der ausgehandelte Schlüssel ist in nachfolgenden Krypto-Operationen (z. B. Test der Zugriffsrechte eines neuen File) nicht verwendbar.

2.164 Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_FF_7)

2.164.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_ECKA_FF_7
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels ECKA nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels ECKA zur Realisierung von Kernroutinen für das Key-Agreement an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.164.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06

2.164.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-OBJECT_DEACTIVATED-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_DEACTIVATED-1	Key-Objekt befindet sich im Zustand "operational state - deactivated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (nicht fehlendes 7c-Tag)

2.164.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_ECKA_FF_7						
CLA	INS	P1	P2	Lc	Data	Le

00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

2.164.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.164.6 Verifikationen

ID	Beschreibung
VF- GENERAL_AUTHENTICATE_ECKA_DH-1	Der ausgehandelte Schlüssel ist in nachfolgenden Krypto-Operationen (z. B. Test der Zugriffsrechte eines neuen File) nicht verwendbar.

2.165 Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_FF_8_1)

2.165.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_ECKA_FF_8_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels ECKA nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt für ECKA-EG mit fehlendem 7c-Tag. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels ECKA zur Realisierung von Kernroutinen für das Key-Agreement an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche

	Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.165.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06

2.165.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-INCORRECT_PARAMETERS-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (fehlendes 7c-Tag)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-UNSUPPORTED_FUNCTION	Schlüssel unterstützt Algorithmus

NCTION-2	
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.165.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_ECKA_FF_8_1						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

2.165.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.165.6 Verifikationen

ID	Beschreibung
VF-GENERAL_AUTHENTICATE_ECKA_DH-1	Der ausgehandelte Schlüssel ist in nachfolgenden Krypto-Operationen (z. B. Test der Zugriffsrechte eines neuen File) nicht verwendbar.

2.166 Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_FF_8_2)

2.166.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_ECKA_FF_8_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels ECKA nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt für ECKA-DH (TLS-Client) mit manipuliertem 06-Tag. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels ECKA zur Realisierung von Kernroutinen für das Key-Agreement an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.166.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06

2.166.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-INCORRECT_PARAMETERS-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (manipuliertes 06-Tag)
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN- NO_KEY_REFEREN CE-2	Key-Objekt ist ausgewählt
CN- KEY_NOT_FOUND- 2	KEY-Objekt kann gefunden werden
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN- UNSUPPORTED_FU NCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID- 2	Key-Daten sind vorhanden
CN- OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.166.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_ECKA_FF_8_2						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

2.166.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.166.6 Verifikationen

ID	Beschreibung
VF- GENERAL_AUTHENTICATE_ECKA_DH-1	Der ausgehandelte Schlüssel ist in nachfolgenden Krypto-Operationen (z. B. Test der Zugriffsrechte eines neuen File) nicht verwendbar.

2.167 Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_FF_8_3)

2.167.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_ECKA_FF_8_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels ECKA nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt für ECKA-DH (TLS-Client) mit manipuliertem 86-Tag. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels ECKA zur Realisierung von Kernroutinen für das Key-Agreement an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.167.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06

2.167.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-INCORRECT_PARAMETERS-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (manipuliertes 86-Tag)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.167.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_ECKA_FF_8_3						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

2.167.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.167.6 Verifikationen

ID	Beschreibung
VF-GENERAL_AUTHENTICATE_ECKA_DH-1	Der ausgehandelte Schlüssel ist in nachfolgenden Krypto-Operationen (z. B. Test der Zugriffsrechte eines neuen File) nicht verwendbar.

2.168 Testfall: GENERAL AUTHENTICATE mittels ECKA (TC_GENERAL_AUTHENTICATE_ECKA_FF_8_4)

2.168.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_ECKA_FF_8_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL

	AUTHENTICATE mittels ECKA nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt für ECKA-DH (TLS-Server) mit manipuliertem 86-Tag. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels ECKA zur Realisierung von Kernroutinen für das Key-Agreement an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.168.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06

2.168.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-INCORRECT_PARAMETERS-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (manipuliertes 86-Tag)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden

CN-SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-UNSUPPORTED_FU NCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID- 2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.168.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_ECKA_FF_8_4						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

2.168.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.168.6 Verifikationen

ID	Beschreibung

VF- GENERAL_AUTHENTICATE_ECKA_DH-1	Der ausgehandelte Schlüssel ist in nachfolgenden Krypto-Operationen (z. B. Test der Zugriffsrechte eines neuen File) nicht verwendbar.

2.169 Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_GF_1_1)

2.169.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_PACE_GF_1_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels PACE erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Die ist der 1. Schritt des PACE-Protokolls. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels PACE zur Realisierung des PACE-Protokolls an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.169.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.169.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-NO_ERROR-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-NO_PIN_REFEREN	PIN-Objekt ist ausgewählt

CE-2	
CN-PIN_NOT_FOUND-2	PIN-Objekt kann gefunden werden
CN-SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN-PIN_INVALID-2	PIN-Daten sind vorhanden
CN-INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 7c)

2.169.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_PACE_GF_1_1						
CLA	INS	P1	P2	Lc	Data	Le
10	86	00	00	02	7c 00	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.169.5 Erwartete Ergebnisse

ID	Beschreibung
RS-F9E8	7c LL [80 LL [XX...XX]] 90 00

2.169.6 Verifikationen

ID	Beschreibung
VF-GENERAL_AUTHENTICATE_PACE-1	Der Sicherheitszustand PACE ist gesetzt und kann nachfolgend erfolgreich genutzt werden.

2.170 Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_GF_1_2)

2.170.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_PACE_GF_1_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels PACE erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Die ist der 2. Schritt des PACE-Protokolls. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels PACE zur Realisierung des PACE-Protokolls an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.170.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.170.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-NO_ERROR-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-NO_PIN_REFERENCE-2	PIN-Objekt ist ausgewählt
CN-PIN_NOT_FOUND-2	PIN-Objekt kann gefunden werden
CN-	Zugriffsregel ist erfüllt

SECURITY_STATU S_NOT_SATISFIED- 2	
CN-PIN_INVALID-2	PIN-Daten sind vorhanden
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 7c)

2.170.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_PACE_GF_1_2						
CLA	INS	P1	P2	Lc	Data	Le
10	86	00	00	LL	7c LL [81 LL [XX...XX]]	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.170.5 Erwartete Ergebnisse

ID	Beschreibung
RS-1AD8	7c LL [82 LL [XX...XX]] 90 00

2.170.6 Verifikationen

ID	Beschreibung
VF-GENERAL_AUTHENTICATE_PACE-1	Der Sicherheitszustand PACE ist gesetzt und kann nachfolgend erfolgreich genutzt werden.

2.171 Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_GF_1_3)

2.171.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_PACE_GF_1_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels PACE erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Die ist der 3. Schritt des PACE-Protokolls. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels PACE zur Realisierung des PACE-Protokolls an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.171.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.171.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-NO_ERROR-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-NO_PIN_REFERENCE-2	PIN-Objekt ist ausgewählt
CN-PIN_NOT_FOUND-2	PIN-Objekt kann gefunden werden
CN-	Zugriffsregel ist erfüllt

SECURITY_STATU S_NOT_SATISFIED- 2	
CN-PIN_INVALID-2	PIN-Daten sind vorhanden
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 7c)

2.171.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_PACE_GF_1_3						
CLA	INS	P1	P2	Lc	Data	Le
10	86	00	00	LL	7c LL [83 LL [XX...XX]]	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.171.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6B08	7c LL [84 LL [XX...XX]] 90 00

2.171.6 Verifikationen

ID	Beschreibung
VF-GENERAL_AUTHENTICATE_PACE-1	Der Sicherheitszustand PACE ist gesetzt und kann nachfolgend erfolgreich genutzt werden.

2.172 Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_GF_1_4)

2.172.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_PACE_GF_1_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels PACE erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Die ist der 4. Schritt des PACE-Protokolls. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels PACE zur Realisierung des PACE-Protokolls an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.172.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.172.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-NO_ERROR-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-NO_PIN_REFERENCE-2	PIN-Objekt ist ausgewählt
CN-PIN_NOT_FOUND-2	PIN-Objekt kann gefunden werden
CN-	Zugriffsregel ist erfüllt

SECURITY_STATU S_NOT_SATISFIED- 2	
CN-PIN_INVALID-2	PIN-Daten sind vorhanden
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 7c)

2.172.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_PACE_GF_1_4						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	7c LL [85 LL [XX...XX]]	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.172.5 Erwartete Ergebnisse

ID	Beschreibung
RS-B810	7c LL [86 LL [XX...XX]] 90 00

2.172.6 Verifikationen

ID	Beschreibung
VF-GENERAL_AUTHENTICATE_PACE-1	Der Sicherheitszustand PACE ist gesetzt und kann nachfolgend erfolgreich genutzt werden.

2.173 Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_GF_2)

2.173.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_PACE_GF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels PACE erfolgreich durchgeführt werden kann und das Protokoll fehlschlägt. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels PACE zur Realisierung des PACE-Protokolls an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.173.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.173.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN- PROTOCOL_ERROR-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN- SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- NO_PIN_REFERENCE-2	PIN-Objekt ist ausgewählt
CN- PIN_NOT_FOUND-2	PIN-Objekt kann gefunden werden
CN-	Zugriffsregel ist erfüllt

SECURITY_STATU S_NOT_SATISFIED- 2	
CN-PIN_INVALID-2	PIN-Daten sind vorhanden
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 7c)

2.173.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_PACE_GF_2						
CLA	INS	P1	P2	Lc	Data	Le
10	86	00	00	02	7c 00	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.173.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6300	Das Testsystem antwortet mit '63 00'.

2.173.6 Verifikationen

ID	Beschreibung
VF-GENERAL_AUTHENTICATE_PACE-1	Der Sicherheitszustand PACE ist gesetzt und kann nachfolgend erfolgreich genutzt werden.

2.174 Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_FF_1)

2.174.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_PACE_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels PACE nicht erfolgreich durchgeführt werden kann, wenn kein PIN-Objekt ausgewählt ist. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels PACE zur Realisierung des PACE-Protokolls an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.174.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.174.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN- NO_PIN_REFEREN CE-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- NO_PIN_REFEREN CE-1	PIN-Objekt ist nicht ausgewählt
CN- PIN_NOT_FOUND-2	PIN-Objekt kann gefunden werden

CN-SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN-PIN_INVALID-2	PIN-Daten sind vorhanden
CN-INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 7c)

2.174.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_PACE_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
10	86	00	00	02	7c 00	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.174.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6985	Das Testsystem antwortet mit '69 85'.

2.174.6 Verifikationen

ID	Beschreibung
VF-GENERAL_AUTHENTICATE_PACE-2	Der Sicherheitszustand PACE ist nicht gesetzt und kann daher nachfolgend nicht genutzt werden.

2.175 Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_FF_2)

2.175.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_PACE_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels PACE nicht erfolgreich durchgeführt werden kann, wenn das PIN-Objekt nicht gefunden werden kann. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels PACE zur Realisierung des PACE-Protokolls an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.175.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.175.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PIN_NOT_FOUND-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-PIN_NOT_FOUND-1	PIN-Objekt kann nicht gefunden werden
CN-NO_PIN_REFERENCE-2	PIN-Objekt ist ausgewählt
CN-	Zugriffsregel ist erfüllt

SECURITY_STATU S_NOT_SATISFIED- 2	
CN-PIN_INVALID-2	PIN-Daten sind vorhanden
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 7c)

2.175.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_PACE_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
10	86	00	00	02	7c 00	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.175.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.175.6 Verifikationen

ID	Beschreibung
VF-GENERAL_AUTHENTICATE_PACE-2	Der Sicherheitszustand PACE ist nicht gesetzt und kann daher nachfolgend nicht genutzt werden.

2.176 Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_FF_3)

2.176.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_PACE_FF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels PACE nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels PACE zur Realisierung des PACE-Protokolls an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.176.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.176.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SECURITY_STATU S_NOT_SATISFIED- 1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATU S_NOT_SATISFIED- 1	Zugriffsregel ist nicht erfüllt
CN-	PIN-Objekt ist ausgewählt

NO_PIN_REFEREN CE-2	
CN- PIN_NOT_FOUND-2	PIN-Objekt kann gefunden werden
CN-PIN_INVALID-2	PIN-Daten sind vorhanden
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 7c)

2.176.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_PACE_FF_3						
CLA	INS	P1	P2	Lc	Data	Le
10	86	00	00	02	7c 00	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.176.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.176.6 Verifikationen

ID	Beschreibung
VF-GENERAL_AUTHENTICATE_PACE-2	Der Sicherheitszustand PACE ist nicht gesetzt und kann daher nachfolgend nicht genutzt werden.

2.177 Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_FF_4)

2.177.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_PACE_FF_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels PACE nicht erfolgreich durchgeführt werden kann, wenn die PIN-Daten nicht vorhanden sind. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels PACE zur Realisierung des PACE-Protokolls an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.177.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.177.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PIN_INVALID-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-PIN_INVALID-1	PIN-Daten sind nicht vorhanden
CN-NO_PIN_REFERENCE-2	PIN-Objekt ist ausgewählt
CN-PIN_NOT_FOUND-2	PIN-Objekt kann gefunden werden

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 7c)

2.177.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_PACE_FF_4						
CLA	INS	P1	P2	Lc	Data	Le
10	86	00	00	02	7c 00	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.177.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6400	Das Testsystem antwortet mit '64 00'.

2.177.6 Verifikationen

ID	Beschreibung
VF-GENERAL_AUTHENTICATE_PACE-2	Der Sicherheitszustand PACE ist nicht gesetzt und kann daher nachfolgend nicht genutzt werden.

2.178 Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_FF_5_1)

2.178.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_PACE_FF_5_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels PACE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 7c. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels PACE zur Realisierung des PACE-Protokolls an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.178.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.178.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-INCORRECT_PARAMETERS-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 7c)
CN-NO_PIN_REFEREN	PIN-Objekt ist ausgewählt

CE-2	
CN-PIN_NOT_FOUND-2	PIN-Objekt kann gefunden werden
CN-SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN-PIN_INVALID-2	PIN-Daten sind vorhanden

2.178.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_PACE_FF_5_1						
CLA	INS	P1	P2	Lc	Data	Le
10	86	00	00	02	ff 00	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.178.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.178.6 Verifikationen

ID	Beschreibung
VF-GENERAL_AUTHENTICATE_PACE-2	Der Sicherheitszustand PACE ist nicht gesetzt und kann daher nachfolgend nicht genutzt werden.

2.179 Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_FF_5_2)

2.179.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_PACE_FF_5_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels PACE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 81 im Protokollschritt 2. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels PACE zur Realisierung des PACE-Protokolls an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.179.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.179.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-INCORRECT_PARAMETERS-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 81 im Protokollschritt 2)
CN-NO_PIN_REFERENCED	PIN-Objekt ist ausgewählt

CE-2	
CN-PIN_NOT_FOUND-2	PIN-Objekt kann gefunden werden
CN-SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN-PIN_INVALID-2	PIN-Daten sind vorhanden

2.179.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_PACE_FF_5_2						
CLA	INS	P1	P2	Lc	Data	Le
10	86	00	00	LL	7c LL [ff LL [XX...XX]]	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.179.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.179.6 Verifikationen

ID	Beschreibung
VF-GENERAL_AUTHENTICATE_PACE-2	Der Sicherheitszustand PACE ist nicht gesetzt und kann daher nachfolgend nicht genutzt werden.

2.180 Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_FF_5_3)

2.180.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_PACE_FF_5_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels PACE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 83 im Protokollschritt 3. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels PACE zur Realisierung des PACE-Protokolls an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.180.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.180.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-INCORRECT_PARAMETERS-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 83 im Protokollschritt 3)
CN-NO_PIN_REFERENCED	PIN-Objekt ist ausgewählt

CE-2	
CN-PIN_NOT_FOUND-2	PIN-Objekt kann gefunden werden
CN-SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN-PIN_INVALID-2	PIN-Daten sind vorhanden

2.180.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_PACE_FF_5_3						
CLA	INS	P1	P2	Lc	Data	Le
10	86	00	00	LL	7c LL [ff LL [XX...XX]]	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.180.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.180.6 Verifikationen

ID	Beschreibung
VF-GENERAL_AUTHENTICATE_PACE-2	Der Sicherheitszustand PACE ist nicht gesetzt und kann daher nachfolgend nicht genutzt werden.

2.181 Testfall: GENERAL AUTHENTICATE mittels PACE (TC_GENERAL_AUTHENTICATE_PACE_FF_5_4)

2.181.1 Informationen

ID	TC_GENERAL_AUTHENTICATE_PACE_FF_5_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERAL AUTHENTICATE mittels PACE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 85 im Protokollschritt 4. Dazu wird eine Kommandonachricht für GENERAL AUTHENTICATE mittels PACE zur Realisierung des PACE-Protokolls an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.181.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.5

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.181.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-INCORRECT_PARAMETERS-1	Es muss vorherig das Kommando MSE (SET-Variante mit AT-Template) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 85 im Protokollschritt 4)
CN-NO_PIN_REFERENCED	PIN-Objekt ist ausgewählt

CE-2	
CN-PIN_NOT_FOUND-2	PIN-Objekt kann gefunden werden
CN-SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN-PIN_INVALID-2	PIN-Daten sind vorhanden

2.181.4 APDU-Kommandos

ID: CM-GENERAL_AUTHENTICATE_PACE_FF_5_4						
CLA	INS	P1	P2	Lc	Data	Le
10	86	00	00	LL	7c LL [ff LL [XX...XX]]	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.181.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.181.6 Verifikationen

ID	Beschreibung
VF-GENERAL_AUTHENTICATE_PACE-2	Der Sicherheitszustand PACE ist nicht gesetzt und kann daher nachfolgend nicht genutzt werden.

2.182 Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_GF_1)

2.182.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.182.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_10, VI_02_06, VI_03_03

2.182.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN- KEY_INITIALIZATI ON-2	Key-Pair-Objekt befindet sich nicht im Zustand "initialization"
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt fehlt nicht)

2.182.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	b6 LL [XX...XX]	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.182.5 Erwartete Ergebnisse

ID	Beschreibung
RS-FEE8	7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 90 00

2.182.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_O UTPUT_ONLY-1	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist erfolgreich und der Schlüssel kann in nachfolgenden Operationen erfolgreich verwendet werden.

2.183 Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_1)

2.183.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.183.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_10, VI_02_06, VI_03_03

2.183.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-KEY_NOT_FOUND-	KEY-Objekt kann gefunden werden

2	
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN- KEY_INITIALIZATI ON-2	Key-Pair-Objekt befindet sich nicht im Zustand "initialization"
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt fehlt nicht)

2.183.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	b6 LL [XX...XX]	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.183.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.183.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_O UTPUT_ONLY-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.184 Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_2)

2.184.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn das KEY-Objekt nicht gefunden wird. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.184.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_10, VI_02_06, VI_03_03

2.184.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	KEY-Objekt kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN- KEY_INITIALIZATI ON-2	Key-Pair-Objekt befindet sich nicht im Zustand "initialization"
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt fehlt nicht)

2.184.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	b6 LL [XX...XX]	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.184.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.184.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_O UTPUT_ONLY-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.185 Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_3_1)

2.185.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_3_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Nicht erfüllt bedeutet in diesem Testfall, dass der notwendige PACE-Kanal nicht aufgebaut ist. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.185.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_10, VI_02_06, VI_03_03

2.185.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt (PACE-Kanal nicht aufgebaut)

CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-KEY_INITIALIZATION-2	Key-Pair-Objekt befindet sich nicht im Zustand "initialization"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt fehlt nicht)

2.185.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_3_1						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	b6 LL [XX...XX]	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.185.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.185.6 Verifikationen

ID	Beschreibung
VF-GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_ONLY-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet

	werden.

2.186 Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_3_2)

2.186.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_3_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Nicht erfüllt bedeutet in diesem Testfall, dass das Key-Pair-Objekt terminiert ist. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.186.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_10, VI_02_06, VI_03_03

2.186.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATU	Zugriffsregel ist nicht erfüllt (Key-Pair-Objekt terminiert)

S_NOT_SATISFIED-1	
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-KEY_INITIALIZATION-2	Key-Pair-Objekt befindet sich nicht im Zustand "initialization"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt fehlt nicht)

2.186.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_3_2						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	b6 LL [XX...XX]	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.186.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.186.6 Verifikationen

ID	Beschreibung
VF-	Das Auslesen des Public-Key aus dem

GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_ONLY-2	entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.187 Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_4)

2.187.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn sich das Key-Pair-Objekt im Zustand "initialization" befindet. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.187.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_10, VI_02_06, VI_03_03

2.187.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN-KEY_INITIALIZATION-1	Key-Pair-Objekt befindet sich im Zustand "initialization"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt fehlt nicht)

2.187.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_4						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	b6 LL [XX...XX]	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.187.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.187.6 Verifikationen

ID	Beschreibung

VF- GENERATE_ASYMMETRIC_KEY_PAIR_O UTPUT_ONLY-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.188 Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_1)

2.188.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt b6 fehlt. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.188.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_10, VI_02_06, VI_03_03

2.188.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN- INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (b6-Objekt fehlt)
CN- INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN- SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN- KEY_INITIALIZATION-2	Key-Pair-Objekt befindet sich nicht im Zustand "initialization"

2.188.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_1						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	00		XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.188.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.188.6 Verifikationen

ID	Beschreibung

VF- GENERATE_ASYMMETRIC_KEY_PAIR_O UTPUT_ONLY-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.189 Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_2)

2.189.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt b6 leer ist. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.189.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_10, VI_02_06, VI_03_03

2.189.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN- SEMANTIC_CORRE	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CTNESS	
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (b6-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_INITIALIZATION-2	Key-Pair-Objekt befindet sich nicht im Zustand "initialization"

2.189.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_2						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	02	b6 00	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.189.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.189.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_ONLY-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.190 Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_3)

2.190.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag b6. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.190.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_10, VI_02_06, VI_03_03

2.190.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für b6)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_INITIALIZATION-2	Key-Pair-Objekt befindet sich nicht im Zustand "initialization"

2.190.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_3						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	05	b6 03 [ff 01 [XX]]	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.190.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.190.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_O UTPUT_ONLY-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.191 Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_4)

2.191.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 84 fehlt. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.191.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_10, VI_02_06, VI_03_03

2.191.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (84-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_INITIALIZATION-2	Key-Pair-Objekt befindet sich nicht im Zustand "initialization"

2.191.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_4						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	02	b6 00	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.191.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.191.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_ONLY-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.192 Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_5)

2.192.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 84 leer ist. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.192.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_10, VI_02_06, VI_03_03

2.192.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (84-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_INITIALIZATION-2	Key-Pair-Objekt befindet sich nicht im Zustand "initialization"

2.192.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_5						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	04	b6 02 [84 00]	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.192.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.192.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_O UTPUT_ONLY-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.193 Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_6)

2.193.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 84. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.193.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_10, VI_02_06, VI_03_03

2.193.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- INCORRECT_PARA METERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 84)
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- KEY_NOT_FOUND- 2	KEY-Objekt kann gefunden werden
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN- KEY_INITIALIZATI ON-2	Key-Pair-Objekt befindet sich nicht im Zustand "initialization"

2.193.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_6						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	05	b6 03 [84 01 [XX...XX]	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.193.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.193.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_O UTPUT_ONLY-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.194 Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_7)

2.194.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_7
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass ein Objekt a4 fälschlicherweise vorhanden ist. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.194.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_10, VI_02_06, VI_03_03

2.194.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (a4-Objekt ist fälschlicherweise vorhanden)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_INITIALIZATION-2	Key-Pair-Objekt befindet sich nicht im Zustand "initialization"

2.194.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_7						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	05	a4 03 [84 01 [XX]]	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.194.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.194.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_O UTPUT_ONLY-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.195 Testfall: GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_8)

2.195.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_8
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass ein Objekt 7f 49 fälschlicherweise vorhanden ist. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR nur Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.195.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_10, VI_02_06, VI_03_03

2.195.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (7f 49-Objekt ist fälschlicherweise vorhanden)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_INITIALIZATION-2	Key-Pair-Objekt befindet sich nicht im Zustand "initialization"

2.195.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_OF_PUBLIC_KEY_ONLY_FF_5_8						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	08	b6 06 [84 01 [XX] 7f 49 00]	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.195.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.195.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_OUTPUT_ONLY-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.196 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_GF_1_1)

2.196.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_GF_1_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein Key-Pair-Objekt für DST (ECDSA ohne Hashing) mit Key-LifecycleStatus 'initialisation'. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.196.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.196.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt ist nicht leer)

2.196.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_GF_1_1						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	15	b6 13 [84 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.196.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.196.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-1	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist erfolgreich und der Schlüssel kann in nachfolgenden Operationen erfolgreich verwendet werden.

2.197 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_GF_1_2)

2.197.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_GF_1_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein Key-Pair-Objekt für DST (ECDSA ohne Hashing) mit Key-LifecycleStatus 'deactivated'. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.197.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.197.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt ist nicht leer)

2.197.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_GF_1_2						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	15	b6 13 [81 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.197.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.197.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-1	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist erfolgreich und der Schlüssel kann in nachfolgenden Operationen erfolgreich verwendet werden.

2.198 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_GF_1_3)

2.198.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_GF_1_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein Key-Pair-Objekt für AT (ECDSA ohne Hashing) mit Key-LifecycleStatus 'initialisation'. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der

	Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.198.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.198.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt ist nicht leer)

2.198.4 APDU-Kommandos

ID: CM-

GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_GF_1_3						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	15	a4 13 [84 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.198.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.198.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-1	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist erfolgreich und der Schlüssel kann in nachfolgenden Operationen erfolgreich verwendet werden.

2.199 Testfall: GENERATE ASYMMETRIC KEY PAIR

Generierung ohne Ausgabe des Public Key

(TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_GF_1_4)

2.199.1 Informationen

ID	Beschreibung
	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_GF_1_4

Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein Key-Pair-Objekt für AT (ECDSA ohne Hashing) mit Key-LifecycleStatus 'deactivated'. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.199.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.199.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

CN- INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt ist nicht leer)

2.199.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_GF_1_4						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	15	a4 13 [84 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.199.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.199.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-1	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist erfolgreich und der Schlüssel kann in nachfolgenden Operationen erfolgreich verwendet werden.

2.200 Testfall: GENERATE ASYMMETRIC KEY PAIR

Generierung ohne Ausgabe des Public Key

(TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_GF_1_5)

2.200.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_GF_1_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein Key-Pair-Objekt für AT (ECKA-EG) mit Key-LifecycleStatus 'initialisation'. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.200.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.200.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-	Key-Pair-Objekt kann gefunden werden

KEY_NOT_FOUND-2	
CN-SECURITY_STATU S_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt ist nicht leer)

2.200.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_P UBLIC_KEY_GF_1_5						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	15	b6 13 [81 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 05 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.200.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.200.6 Verifikationen

ID	Beschreibung

VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-1	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist erfolgreich und der Schlüssel kann in nachfolgenden Operationen erfolgreich verwendet werden.

2.201 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_GF_1_6)

2.201.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_GF_1_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein Key-Pair-Objekt für AT (ECKA-EG) mit Key-LifecycleStatus 'deactivated'. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.201.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.201.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN- SEMANTIC_CORRE	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CTNESS	
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt ist nicht leer)

2.201.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_GF_1_6						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	15	b6 13 [81 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 05 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.201.5 Erwartete Ergebnisse

ID	Beschreibung

RS-9000	Das Testsystem antwortet mit '90 00'.

2.201.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-1	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist erfolgreich und der Schlüssel kann in nachfolgenden Operationen erfolgreich verwendet werden.

2.202 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_GF_1_7)

2.202.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_GF_1_7
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein Key-Pair-Objekt für AT (ECKA-DH) mit Key-LifecycleStatus 'initialisation'. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.202.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.202.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt ist nicht leer)

2.202.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_GF_1_7						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	15	b6 13 [81 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 05 02]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template

bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.202.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.202.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-1	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist erfolgreich und der Schlüssel kann in nachfolgenden Operationen erfolgreich verwendet werden.

2.203 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_GF_1_8)

2.203.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_GF_1_8
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein Key-Pair-Objekt für AT (ECKA-DH) mit Key-LifecycleStatus 'deactivated'. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.203.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.203.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt ist nicht leer)

2.203.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_GF_1_8						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	15	b6 13 [81 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 05 02]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.203.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.203.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-1	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist erfolgreich und der Schlüssel kann in nachfolgenden Operationen erfolgreich verwendet werden.

2.204 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_1)

2.204.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit

	der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.204.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.204.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt ist nicht leer)

2.204.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_1

CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	15	b6 13 [84 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.204.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.204.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-2	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.205 Testfall: GENERATE ASYMMETRIC KEY PAIR

Generierung ohne Ausgabe des Public Key

(TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_2_1)

2.205.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_2_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn das Key-Pair-Objekt für DST nicht

	gefunden wird. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.205.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.205.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	Key-Pair-Objekt für DST kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt ist nicht leer)

2.205.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_2_1						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	15	b6 13 [81 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.205.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.205.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-2	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.206 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_2_2)

2.206.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_2_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn das Key-Pair-Objekt für AT nicht gefunden wird. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.206.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.206.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	Key-Pair-Objekt für AT kann nicht gefunden werden
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN-SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED- 2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt ist nicht leer)

2.206.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_P UBLIC_KEY_FF_2_2						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	15	a4 13 [81 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.206.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.206.6 Verifikationen

ID	Beschreibung
VF-	Ein nachfolgendes Auslesen des Public-Key aus

GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-2	dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.207 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_2_3)

2.207.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_2_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn das Key-Pair-Objekt für AT nicht gefunden wird. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.207.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.207.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN-KEY_NOT_FOUND-1	Key-Pair-Objekt für AT kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt ist nicht leer)

2.207.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_2_3						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	15	a4 13 [81 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 05 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.207.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.207.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-2	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.208 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_2_4)

2.208.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_2_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn das Key-Pair-Objekt für AT nicht gefunden wird. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.208.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.208.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- KEY_NOT_FOUND- 1	Key-Pair-Objekt für AT kann nicht gefunden werden
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN- KEY_ACTIVATED- 2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt ist nicht leer)

2.208.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_P UBLIC_KEY_FF_2_4						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	15	a4 13 [81 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 05 02]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.208.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.208.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-2	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.209 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_3_1)

2.209.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_3_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Nicht erfüllt bedeutet in diesem Testfall, dass der notwendige PACE-Kanal nicht aufgebaut ist. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.209.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.209.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt (PACE-Kanal nicht aufgebaut)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt ist nicht leer)

2.209.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_3_1						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	15	b6 13 [84 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.209.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.209.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-2	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.210 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_3_2)

2.210.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_3_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Nicht erfüllt bedeutet in diesem Testfall, dass das Key-Pair-Objekt terminiert ist. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur

	die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.210.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.210.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt (Key-Pair-Objekt terminiert)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt ist nicht leer)

2.210.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_P

UBLIC_KEY_FF_3_2						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	15	b6 13 [84 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.210.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.210.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-2	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.211 Testfall: GENERATE ASYMMETRIC KEY PAIR

Generierung ohne Ausgabe des Public Key

(TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_4)

2.211.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC

	KEY PAIR Generierung ohne Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn sich das Key-Pair-Objekt im Zustand "operational state - activated" befindet. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.211.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.211.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_ACTIVATED-1	Key-Pair-Objekt befindet sich im Zustand "operational state - activated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-INCORRECT_PARAMETERS	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt ist nicht leer)

METERS-2	

2.211.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_4						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	15	b6 13 [84 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.211.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.211.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-2	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.212 Testfall: GENERATE ASYMMETRIC KEY PAIR

Generierung ohne Ausgabe des Public Key

(TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_1)

2.212.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt b6 leer ist. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.212.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.212.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (b6-Objekt ist leer)
CN-	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

INSTRUCTION_NOT_SUPPORTED-2	
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.212.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_1						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	02	b6 00	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.212.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.212.6 Verifikationen

ID	Beschreibung
VF-	Ein nachfolgendes Auslesen des Public-Key aus

GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-2	dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.213 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_2)

2.213.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag b6. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.213.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.213.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN- INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für b6)
CN- INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN- SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN- KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.213.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_2						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	15	b6 13 [ff 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.213.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.213.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-2	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.214 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_3)

2.214.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt b6 fehlt. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.214.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.214.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (b6-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.214.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_3						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	00		--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.214.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.214.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-2	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.215 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_4)

2.215.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 84 leer ist. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.215.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.215.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (84-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.215.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_4						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	14	b6 12 [84 00 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für

ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.215.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.215.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-2	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.216 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_5)

2.216.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 84. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.

Klassifizierung	Fehlerfall-Test

2.216.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.216.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 84)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.216.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_5						
CLA	INS	P1	P2	Lc	Data	Le

00	47	86	00	15	b6 13 [84 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.216.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.216.6 Verifikationen

ID	Beschreibung
VF-GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-2	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.217 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_6)

2.217.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 84

	fehlt. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.217.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.217.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (84-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.217.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_6						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	12	b6 10 [7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.217.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.217.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-2	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.218 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_7)

2.218.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_7
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt a4 leer ist. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.218.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.218.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (a4-Objekt ist leer)
CN-	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

INSTRUCTION_NOT_SUPPORTED-2	
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.218.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_7						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	02	a4 00	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.218.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.218.6 Verifikationen

ID	Beschreibung
VF-	Ein nachfolgendes Auslesen des Public-Key aus

GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-2	dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.219 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_8)

2.219.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_8
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag a4. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.219.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.219.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN- INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für a4)
CN- INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN- SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN- KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.219.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_8						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	15	a4 13 [ff 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.219.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.219.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-2	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.220 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_9)

2.220.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_9
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt a4 fehlt. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.220.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.220.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (a4-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.220.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_9						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	00		--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.220.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.220.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-2	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.221 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_10)

2.221.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_10
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 84 fehlt. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.221.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.221.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (84-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.221.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_10						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	12	a4 10 [7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für

ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.221.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.221.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-2	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.222 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_11)

2.222.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_11
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 84 leer ist. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.

Klassifizierung	Fehlerfall-Test

2.222.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.222.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- INCORRECT_PARA METERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (84-Objekt ist leer)
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- KEY_NOT_FOUND- 2	Key-Pair-Objekt kann gefunden werden
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN- KEY_ACTIVATED- 2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.222.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_P UBLIC_KEY_FF_5_11						
CLA	INS	P1	P2	Lc	Data	Le

00	47	86	00	15	a4 13 [84 00 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.222.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.222.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-2	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.223 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_12)

2.223.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_12
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 84. Dazu wird

	eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.223.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.223.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 84)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.223.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_12						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	15	a4 13 [84 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.223.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.223.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-2	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.224 Testfall: GENERATE ASYMMETRIC KEY PAIR

Generierung ohne Ausgabe des Public Key

(TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_13)

2.224.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_13
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 06 leer ist. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.224.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.224.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (06-Objekt ist leer)
CN-	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

INSTRUCTION_NOT_SUPPORTED-2	
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.224.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_13						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	10	b6 08 [84 01 [XX] 7f 49 02 [06 00]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.224.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.224.6 Verifikationen

ID	Beschreibung
VF-	Ein nachfolgendes Auslesen des Public-Key aus

GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-2	dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.225 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_14)

2.225.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_14
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 06 fehlt. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.225.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.225.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN- INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (06-Objekt fehlt)
CN- INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN- SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN- KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.225.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_14						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	08	b6 06 [84 01 [XX] 7f 49 00	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.225.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.225.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-2	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.226 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_15)

2.226.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_15
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falscher OID. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung ohne Ausgabe des Public Key zur Befüllung von persistenten Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.226.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_05

2.226.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falscher OID)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.226.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_15						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	15	b6 13 [84 01 [XX] 7f 49 0d [06 0b [ff ff ff ff ff ff ff ff ff ff ff ff]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

2.226.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.226.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITHOUT_PUBLIC_KEY_OUTPUT-2	Ein nachfolgendes Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.227 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_1)

2.227.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein Key-Pair-Objekt für DST (ECDSA ohne Hashing) mit Key-LifecycleStatus 'initialisation'. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.227.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.227.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt fehlt nicht)

2.227.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_1						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	15	b6 13 [84 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.227.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.227.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-1	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist erfolgreich und der Schlüssel kann in nachfolgenden Operationen erfolgreich verwendet werden.

2.228 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_2)

2.228.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein Key-Pair-Objekt für DST (ECDSA ohne Hashing) mit Key-LifecycleStatus 'deactivated'. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR

	Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.228.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.228.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt fehlt nicht)

2.228.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_2						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	15	b6 13 [81 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.228.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.228.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-1	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist erfolgreich und der Schlüssel kann in nachfolgenden Operationen erfolgreich verwendet werden.

2.229 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_3)

2.229.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein Key-Pair-Objekt für AT (ECDSA ohne Hashing) mit Key-LifecycleStatus 'initialisation'. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.229.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.229.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATU S_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt fehlt nicht)

2.229.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_3						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	15	a4 13 [84 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.229.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.229.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-1	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist erfolgreich und der Schlüssel kann in nachfolgenden Operationen erfolgreich verwendet werden.

2.230 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_4)

2.230.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein Key-Pair-Objekt für AT (ECDSA ohne Hashing) mit Key-LifecycleStatus 'deactivated'. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.230.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.230.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt fehlt nicht)

2.230.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_4						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	15	a4 13 [84 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.230.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.230.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-1	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist erfolgreich und der Schlüssel kann in nachfolgenden Operationen erfolgreich verwendet werden.

2.231 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_5)

2.231.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein Key-Pair-Objekt für AT (ECKA-EG) mit Key-LifecycleStatus 'initialisation'. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.231.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.231.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt fehlt nicht)

2.231.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_5						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	15	b6 13 [81 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 05 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für

ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.231.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.231.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-1	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist erfolgreich und der Schlüssel kann in nachfolgenden Operationen erfolgreich verwendet werden.

2.232 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_6)

2.232.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein Key-Pair-Objekt für AT (ECKA-EG) mit Key-LifecycleStatus 'deactivated'. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.

Klassifizierung	Gutfall-Test

2.232.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.232.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt fehlt nicht)

2.232.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_6						
CLA	INS	P1	P2	Lc	Data	Le

00	47	82	00	15	b6 13 [81 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 05 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.232.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.232.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-1	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist erfolgreich und der Schlüssel kann in nachfolgenden Operationen erfolgreich verwendet werden.

2.233 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_7)

2.233.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_7
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen

	erfüllt sind. Dies betrifft ein Key-Pair-Objekt für AT (ECKA-DH) mit Key-LifecycleStatus 'initialisation'. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.233.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.233.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt fehlt nicht)

2.233.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_7						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	15	b6 13 [81 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 05 02]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.233.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.233.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-1	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist erfolgreich und der Schlüssel kann in nachfolgenden Operationen erfolgreich verwendet werden.

2.234 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_8)

2.234.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_8
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft ein Key-Pair-Objekt für AT (ECKA-DH) mit Key-LifecycleStatus 'deactivated'. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.234.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.234.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-	Key-Pair-Objekt kann gefunden werden

KEY_NOT_FOUND-2	
CN-SECURITY_STATU S_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt fehlt nicht)

2.234.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_8						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	15	b6 13 [81 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 05 02]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.234.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.234.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-1	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist erfolgreich und der Schlüssel kann in nachfolgenden Operationen erfolgreich verwendet werden.

2.235 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_9)

2.235.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_9
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dies betrifft temporäres Key-Pair-Objekt für ECKA-DH. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.235.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.235.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt fehlt nicht)

2.235.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_GF_1_9						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	15	b6 13 [84 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 05 01]]]	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.235.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.235.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-1	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist erfolgreich und der Schlüssel kann in nachfolgenden Operationen erfolgreich verwendet werden.

2.236 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_1)

2.236.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.236.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.236.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt fehlt nicht)

2.236.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	15	b6 13 [84 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu

generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'
Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.236.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.236.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.237 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_2_1)

2.237.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_2_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn das Key-Pair-Objekt für AT nicht gefunden wird. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.237.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.237.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	Key-Pair-Objekt für AT kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt fehlt nicht)

2.237.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_2_1						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	15	b6 13 [84 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.237.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.237.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.238 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_2_2)

2.238.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_2_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn das Key-Pair-Objekt für AT nicht gefunden wird. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur

	Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.238.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.238.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	Key-Pair-Objekt für AT kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt fehlt nicht)

2.238.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_2_2						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	15	b6 13 [84 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.238.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.238.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.239 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_2_3)

2.239.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_2_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn das Key-Pair-Objekt für AT nicht gefunden wird. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.239.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.239.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	Key-Pair-Objekt für AT kann nicht gefunden werden
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN-SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED- 2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt fehlt nicht)

2.239.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLI C_KEY_FF_2_3						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	15	b6 13 [84 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.239.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.239.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.240 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_2_4)

2.240.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_2_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn das Key-Pair-Objekt für AT nicht gefunden wird. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.240.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.240.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	Key-Pair-Objekt für AT kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt fehlt nicht)

2.240.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_2_4						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	15	b6 13 [81 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 05 02]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.240.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.240.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.241 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_3_1)

2.241.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_3_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Nicht erfüllt bedeutet in diesem Testfall, dass der notwendige PACE-Kanal nicht aufgebaut ist. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.241.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.241.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt (PACE-Kanal nicht aufgebaut)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt fehlt nicht)

2.241.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_3_1						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	15	b6 13 [84 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.241.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.241.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.242 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_3_2)

2.242.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_3_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Nicht erfüllt bedeutet in diesem Testfall, dass das Key-Pair-Objekt terminiert ist. Dazu wird eine Kommandonachricht für

	GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.242.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.242.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt (Key-Pair-Objekt terminiert)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt fehlt nicht)

2.242.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_3_2						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	15	b6 13 [84 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.242.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.242.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.243 Testfall: GENERATE ASYMMETRIC KEY PAIR

Generierung mit Ausgabe des Public Key

(TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_4)

2.243.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn sich das Key-Pair-Objekt im Zustand "operational state - activated" befindet. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.243.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.243.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_ACTIVATED-1	Key-Pair-Objekt befindet sich im Zustand "operational state - activated"
CN-	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

INSTRUCTION_NOT_SUPPORTED-2	
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (b6-Objekt fehlt nicht)

2.243.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_4						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	15	b6 13 [84 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.243.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.243.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.244 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_1)

2.244.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt b6 fehlt. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.244.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.244.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (b6-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.244.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_1						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	00		--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.244.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.244.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.245 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_2)

2.245.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt b6 leer ist. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.245.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.245.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (b6-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.245.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_2						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	02	b6 00	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT):

'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.245.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.245.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.246 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_3)

2.246.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag b6. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.

Klassifizierung	Fehlerfall-Test

2.246.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.246.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für b6)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.246.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_3						
CLA	INS	P1	P2	Lc	Data	Le

00	47	82	00	03	b6 13 [ff 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.246.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.246.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.247 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_4)

2.247.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key nicht erfolgreich

	durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 84 fehlt. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.247.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.247.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (84-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.247.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_4						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	12	b6 10 [7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.247.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.247.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.248 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_5)

2.248.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 84 leer ist. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.248.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.248.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (84-Objekt ist leer)
CN-	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

INSTRUCTION_NOT_SUPPORTED-2	
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.248.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_5						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	14	b6 12 [84 00 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.248.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.248.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.249 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_6)

2.249.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 84. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.249.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.249.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 84)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.249.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_6						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	15	b6 13 [84 01 [XX...XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.249.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.249.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.250 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_7)

2.250.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_7
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt a4 leer ist. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.250.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.250.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (a4-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.250.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_7						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	02	a4 00	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT):

'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.250.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.250.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.251 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_8)

2.251.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_8
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag a4. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.

Klassifizierung	Fehlerfall-Test

2.251.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.251.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für a4)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.251.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_8						
CLA	INS	P1	P2	Lc	Data	Le

00	47	82	00	15	a4 13 [ff 01 [XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.251.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.251.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.252 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_9)

2.252.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_9
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key nicht erfolgreich

	durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt a4 fehlt. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.252.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.252.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (a4-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.252.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_9						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	00		--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.252.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.252.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.253 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_10)

2.253.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITHOUT_OUTPUT_OF_PUBLIC_KEY_FF_5_10
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 84 fehlt. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.253.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.253.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (84-Objekt fehlt)
CN-	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

INSTRUCTION_NO T_SUPPORTED-2	
CN- KEY_NOT_FOUND- 2	Key-Pair-Objekt kann gefunden werden
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN- KEY_ACTIVATED- 2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.253.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLI C_KEY_FF_5_10						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	02	a4 00	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.253.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.253.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.254 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_11)

2.254.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_11
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 84 leer ist. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.254.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.254.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (84-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.254.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_11						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	14	a4 12 [84 00 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.254.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.254.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.255 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_12)

2.255.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_12
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 84. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.255.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.255.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 84)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.255.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_12						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	14	a4 13 [84 01 [XX...XX] 7f 49 0d [06 0b [06 09 04 00 7f 00 07 01 01 04 01]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für

ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.255.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.255.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.256 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_13)

2.256.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_13
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 06 leer ist. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit

	der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.256.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.256.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (06-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.256.4 APDU-Kommandos

ID: CM-GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_13

CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	10	b6 08 [84 01 [XX] 7f 49 0d [06 00]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.256.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.256.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.257 Testfall: GENERATE ASYMMETRIC KEY PAIR

Generierung mit Ausgabe des Public Key

(TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_14)

2.257.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_14
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC

	KEY PAIR Generierung mit Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 06 fehlt. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.257.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.257.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (06-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	Key-Pair-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN-KEY_ACTIVATED-	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2

2.257.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_14						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	08	b6 06 [84 01 [XX] 7f 49 0d	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.257.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.257.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WITH_PUBLIC_KEY_OUTPUT-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.258 Testfall: GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key (TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_15)

2.258.1 Informationen

ID	TC_GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLIC_KEY_FF_5_15
Beschreibung	Dieser Test verifiziert, dass ein Kommando GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falscher OID. Dazu wird eine Kommandonachricht für GENERATE ASYMMETRIC KEY PAIR Generierung mit Ausgabe des Public Key zur Befüllung von persistenten und temporären Key-Objekten mit Schlüsseldaten an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.258.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_09a, PN_05_06, VI_02_05

2.258.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falscher OID)
CN-	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

INSTRUCTION_NO T_SUPPORTED-2	
CN- KEY_NOT_FOUND- 2	Key-Pair-Objekt kann gefunden werden
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt (PACE-Kanal aufgebaut)
CN- KEY_ACTIVATED- 2	Key-Pair-Objekt befindet sich nicht im Zustand "operational state - activated"

2.258.4 APDU-Kommandos

ID: CM- GENERATE_ASYMMETRIC_KEY_PAIR_GENERATION_WITH_OUTPUT_OF_PUBLI C_KEY_FF_5_15						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	15	b6 13 [84 01 [XX] 7f 49 0d [06 0b [ff ff ff ff ff ff ff ff ff ff ff]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.258.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.258.6 Verifikationen

ID	Beschreibung
VF- GENERATE_ASYMMETRIC_KEY_PAIR_WI TH_PUBLIC_KEY_OUTPUT-2	Das Auslesen des Public-Key aus dem entsprechenden Key-Pair-Objekt ist nicht erfolgreich und der Schlüssel kann daher nicht in nachfolgenden Operationen verwendet werden.

2.259 Testfall: GET CHALLENGE (TC_GET_CHALLENGE_GF_1)

2.259.1 Informationen

ID	TC_GET_CHALLENGE_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando GET CHALLENGE erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für GET CHALLENGE zur Verwendung von Zufallszahlen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.259.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.7.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02, PN_05_01, PN_05_11

2.259.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

INSTRUCTION_NO T_SUPPORTED-2	

2.259.4 APDU-Kommandos

ID: CM-GET_CHALLENGE_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	84	0X	00	--	--	XX

'P1' enthält '00': generierte Zufallszahl wird intern gespeichert '01': generierte Zufallszahl wird intern nicht gespeichert.

'Le' enthält die Anzahl der Oktette zu erwartenden Zufallszahl (Hersteller-abhängig und in Abhängigkeit vom Ausgabeformat).

2.259.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.259.6 Verifikationen

ID	Beschreibung
VF-GET_CHALLENGE-1	Es wird eine Zufallszahl zurückgegeben.

2.260 Testfall: GET CHALLENGE (TC_GET_CHALLENGE_FF_1)

2.260.1 Informationen

ID	TC_GET_CHALLENGE_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando GET CHALLENGE nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für GET CHALLENGE zur Verwendung von Zufallszahlen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird

	im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.260.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.7.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02, PN_05_01, PN_05_11

2.260.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"

2.260.4 APDU-Kommandos

ID: CM-GET_CHALLENGE_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	84	0X	00	--	--	XX

'P1' enthält '00': generierte Zufallszahl wird intern gespeichert '01': generierte Zufallszahl wird intern nicht gespeichert.

'Le' enthält die Anzahl der Oktette zu erwartenden Zufallszahl (Hersteller-abhängig und in Abhängigkeit vom Ausgabeformat).

2.260.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.260.6 Verifikationen

ID	Beschreibung
VF-GET_CHALLENGE-2	Es wird keine Zufallszahl zurückgegeben.

2.261 Testfall: INTERNAL AUTHENTICATE (TC_INTERNAL_AUTHENTICATE_GF_1)

2.261.1 Informationen

ID	TC_INTERNAL_AUTHENTICATE_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando INTERNAL AUTHENTICATE erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Die Durchführung erfolgt für ECDSA ohne Hashing. Dazu wird eine Kommandonachricht für INTERNAL AUTHENTICATE zur internen Authentisierung an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.261.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.7

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_03, VI_02_10

2.261.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-NO_ERROR-1	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Key-Pair-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.261.4 APDU-Kommandos

ID: CM-INTERNAL_AUTHENTICATE_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.261.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.261.6 Verifikationen

ID	Beschreibung
VF-INTERNAL_AUTHENTICATE-1	Die zurückgegebene Signatur der Eingabedaten kann erfolgreich in nachfolgenden Operationen verwendet werden.

2.262 Testfall: INTERNAL AUTHENTICATE (TC_INTERNAL_AUTHENTICATE_FF_1)

2.262.1 Informationen

ID	TC_INTERNAL_AUTHENTICATE_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando INTERNAL AUTHENTICATE nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für INTERNAL AUTHENTICATE zur internen Authentisierung an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.262.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.7

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_03, VI_02_10

2.262.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-INSTRUCTION_NO T_SUPPORTED-1	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Key-Pair-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.262.4 APDU-Kommandos

ID: CM-INTERNAL_AUTHENTICATE_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.262.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.262.6 Verifikationen

ID	Beschreibung
VF-INTERNAL_AUTHENTICATE-2	Es wird keine Signatur zurückgegeben.

2.263 Testfall: INTERNAL AUTHENTICATE (TC_INTERNAL_AUTHENTICATE_FF_2)

2.263.1 Informationen

ID	TC_INTERNAL_AUTHENTICATE_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando INTERNAL AUTHENTICATE nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt nicht ausgewählt ist. Dazu wird eine Kommandonachricht für INTERNAL AUTHENTICATE zur internen Authentisierung an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.263.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.7

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_03, VI_02_10

2.263.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-NO_KEY_REFERENC-1	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Key-Pair-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-	Key-Objekt ist nicht ausgewählt

NO_KEY_REFEREN CE-1	
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- KEY_NOT_FOUND- 2	KEY-Objekt kann gefunden werden
CN- UNSUPPORTED_FU NCTION-2	Schlüssel unterstützt Algorithmus
CN- OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.263.4 APDU-Kommandos

ID: CM-INTERNAL_AUTHENTICATE_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.263.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6985	Das Testsystem antwortet mit '69 85'.

2.263.6 Verifikationen

ID	Beschreibung
VF-INTERNAL_AUTHENTICATE-2	Es wird keine Signatur zurückgegeben.

2.264 Testfall: INTERNAL AUTHENTICATE (TC_INTERNAL_AUTHENTICATE_FF_3)

2.264.1 Informationen

ID	TC_INTERNAL_AUTHENTICATE_FF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando INTERNAL AUTHENTICATE nicht erfolgreich durchgeführt werden kann, wenn das KEY-Objekt nicht gefunden wird. Dazu wird eine Kommandonachricht für INTERNAL AUTHENTICATE zur internen Authentisierung an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.264.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.7

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_03, VI_02_10

2.264.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-KEY_NOT_FOUND-1	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Key-Pair-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-	KEY-Objekt kann nicht gefunden werden

KEY_NOT_FOUND-1	
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.264.4 APDU-Kommandos

ID: CM-INTERNAL_AUTHENTICATE_FF_3						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.264.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.264.6 Verifikationen

ID	Beschreibung
VF-INTERNAL_AUTHENTICATE-2	Es wird keine Signatur zurückgegeben.

2.265 Testfall: INTERNAL AUTHENTICATE (TC_INTERNAL_AUTHENTICATE_FF_4)

2.265.1 Informationen

ID	TC_INTERNAL_AUTHENTICATE_FF_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando INTERNAL AUTHENTICATE nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Dazu wird eine Kommandonachricht für INTERNAL AUTHENTICATE zur internen Authentisierung an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.265.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.7

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_03, VI_02_10

2.265.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-UNSUPPORTED_FUNCTION-1	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Key-Pair-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-	Schlüssel unterstützt Algorithmus nicht

UNSUPPORTED_FUNCTION-1	
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.265.4 APDU-Kommandos

ID: CM-INTERNAL_AUTHENTICATE_FF_4						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.265.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.265.6 Verifikationen

ID	Beschreibung
VF-INTERNAL_AUTHENTICATE-2	Es wird keine Signatur zurückgegeben.

2.266 Testfall: INTERNAL AUTHENTICATE (TC_INTERNAL_AUTHENTICATE_FF_5)

2.266.1 Informationen

ID	TC_INTERNAL_AUTHENTICATE_FF_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando INTERNAL AUTHENTICATE nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Dazu wird eine Kommandonachricht für INTERNAL AUTHENTICATE zur internen Authentisierung an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.266.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.7

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_03, VI_02_10

2.266.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-OBJECT_DEACTIVATED-1	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Key-Pair-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN- OBJECT_DEACTIVATED-1	Key-Objekt befindet sich im Zustand "operational state - deactivated"
CN- INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN- KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN- UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN- SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.266.4 APDU-Kommandos

ID: CM-INTERNAL_AUTHENTICATE_FF_5						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.266.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.266.6 Verifikationen

ID	Beschreibung
VF-INTERNAL_AUTHENTICATE-2	Es wird keine Signatur zurückgegeben.

2.267 Testfall: INTERNAL AUTHENTICATE (TC_INTERNAL_AUTHENTICATE_FF_6)

2.267.1 Informationen

ID	TC_INTERNAL_AUTHENTICATE_FF_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando INTERNAL AUTHENTICATE nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Dazu wird eine Kommandonachricht für INTERNAL AUTHENTICATE zur internen Authentisierung an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.267.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.7

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_03, VI_02_10

2.267.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SECURITY_STATU S_NOT_SATISFIED- 1	Es muss das Kommando MSE (SET-Variante mit AT-Template, Übergabe der Key Reference des zugehörigen Key-Pair-Objektes) abgesetzt worden sein.
CN-SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN- SECURITY_STATU S_NOT_SATISFIED- 1	Zugriffsregel ist nicht erfüllt
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- NO_KEY_REFEREN CE-2	Key-Objekt ist ausgewählt
CN- KEY_NOT_FOUND- 2	KEY-Objekt kann gefunden werden
CN- UNSUPPORTED_FU NCTION-2	Schlüssel unterstützt Algorithmus
CN- OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.267.4 APDU-Kommandos

ID: CM-INTERNAL_AUTHENTICATE_FF_6						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.267.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.267.6 Verifikationen

ID	Beschreibung
VF-INTERNAL_AUTHENTICATE-2	Es wird keine Signatur zurückgegeben.

2.268 Testfall: MANAGE CHANNEL (TC_MANAGE_CHANNEL_GF_1)

2.268.1 Informationen

ID	TC_MANAGE_CHANNEL_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MANAGE CHANNEL erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für MANAGE CHANNEL zum Zurücksetzen der Applikationsebene an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.268.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.10.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_23

2.268.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

2.268.4 APDU-Kommandos

ID: CM-MANAGE_CHANNEL_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	70	40	01	--	--	--

2.268.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.268.6 Verifikationen

ID	Beschreibung
VF-MANAGE_CHANNEL-1	Das MF kann nachfolgend ohne vorherige Selektierung benutzt werden und es sind keine bestehenden sicheren Kanäle mehr vorhanden.

2.269 Testfall: MANAGE CHANNEL (TC_MANAGE_CHANNEL_FF_1)

2.269.1 Informationen

ID	TC_MANAGE_CHANNEL_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MANAGE CHANNEL nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für MANAGE CHANNEL zum Zurücksetzen der Applikationsebene an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.269.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.10.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_23

2.269.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"

2.269.4 APDU-Kommandos

ID: CM-MANAGE_CHANNEL_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	70	40	01	--	--	--

2.269.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.269.6 Verifikationen

ID	Beschreibung
VF-MANAGE_CHANNEL-2	Das MF kann ohne vorherige Selektierung nicht benutzt werden und bestehende sichere Kanäle sind weiterhin vorhanden.

2.270 Testfall: MSE RESTORE (TC_MSE_RESTORE_GF_1)

2.270.1 Informationen

ID	TC_MSE_RESTORE_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE RESTORE erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für MSE RESTORE zur Auswahl des SE oder Änderung der aktuell ausgewählten SEID an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.270.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_01_01, VI_01_01

2.270.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

2.270.4 APDU-Kommandos

ID: CM-MSE_RESTORE_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	22	f3	XX	--	--	--

'P2' enthält den SEID.

2.270.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.270.6 Verifikationen

ID	Beschreibung
VF-MSE_RESTORE-1	Das entsprechende SE ist ausgewählt und gesetzt.

2.271 Testfall: MSE RESTORE (TC_MSE_RESTORE_FF_1)

2.271.1 Informationen

ID	TC_MSE_RESTORE_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE RESTORE nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für MSE RESTORE zur Auswahl des SE oder Änderung der aktuell ausgewählten SEID an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.271.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_01_01, VI_01_01

2.271.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRE	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CTNESS	
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"

2.271.4 APDU-Kommandos

ID: CM-MSE_RESTORE_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	22	f3	XX	--	--	--

'P2' enthält den SEID.

2.271.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.271.6 Verifikationen

ID	Beschreibung
VF-MSE_RESTORE-2	Das entsprechende SE ist nicht ausgewählt und nicht gesetzt.

2.272 Testfall: MSE SET mit CRT AT für externe Authentisierung (TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_GF_1)

2.272.1 Informationen

ID	TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für externe Authentisierung erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für externe Authentisierung zum Setzen von Parametern der SE an das

	Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.272.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.272.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 80)

2.272.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	a4	LL	80 0b [0a 04 00 7f 00 07 01 01 04 01 03] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
|| '83-L83-Key Reference' (für das Public Key-Objekt)

2.272.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.272.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION-1	Nachfolgende Krypto-Operationen können ohne MSE-SET-bezogene Fehler erfolgreich ausgeführt werden.

2.273 Testfall: MSE SET mit CRT AT für externe Authentisierung (TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_1)

2.273.1 Informationen

ID	TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für externe Authentisierung nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für externe Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird

	im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.273.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.273.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 80)

2.273.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	a4	LL	80 0b [0a 04 00 7f 00 07 01 01 04 01 03] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
|| '83-L83-Key Reference' (für das Public Key-Objekt)

2.273.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.273.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.274 Testfall: MSE SET mit CRT AT für externe Authentisierung (TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_2)

2.274.1 Informationen

ID	TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für externe Authentisierung nicht erfolgreich durchgeführt werden kann, wenn das KEY-Objekt nicht gefunden wird. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für externe Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird

	im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.274.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.274.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	KEY-Objekt kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 80)

2.274.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	a4	LL	80 LL [XX...XX] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.274.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.274.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.275 Testfall: MSE SET mit CRT AT für externe Authentisierung (TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_3_1)

2.275.1 Informationen

ID	TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_3_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für externe Authentisierung nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für ECDSA mit SHA256. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für externe Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.

Klassifizierung	Fehlerfall-Test

2.275.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.275.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 80)

2.275.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_3_1

CLA	INS	P1	P2	Lc	Data	Le
00	22	81	a4	LL	80 0b [0a 04 00 7f 00 07 01 01 04 01 03] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
|| '83-L83-Key Reference' (für das Public Key-Objekt)

2.275.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.275.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_EXTERNAL_AUTHENTICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.276 Testfall: MSE SET mit CRT AT für externe Authentisierung (TC_MSE_SET_CERT_AT_EXTERNAL_AUTHENTICATION_FF_3_2)

2.276.1 Informationen

ID	TC_MSE_SET_CERT_AT_EXTERNAL_AUTHENTICATION_FF_3_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für externe Authentisierung nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für ECDSA mit SHA384. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für externe Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.276.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.276.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 80)

2.276.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_3_2						
CLA	INS	P1	P2	Lc	Data	Le

00	22	81	a4	LL	80 0b [0a 04 00 7f 00 07 01 01 04 01 04] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
|| '83-L83-Key Reference' (für das Public Key-Objekt)

2.276.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.276.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_EXTERNAL_AUTHENTICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.277 Testfall: MSE SET mit CERT AT für externe Authentisierung (TC_MSE_SET_CERT_AT_EXTERNAL_AUTHENTICATION_FF_3_3)

2.277.1 Informationen

ID	TC_MSE_SET_CERT_AT_EXTERNAL_AUTHENTICATION_FF_3_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CERT AT für externe Authentisierung nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für ECDSA mit SHA512. Dazu wird eine Kommandonachricht für MSE SET mit CERT AT für externe Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.277.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.277.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 80)

2.277.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_3_3						
CLA	INS	P1	P2	Lc	Data	Le

00	22	81	a4	LL	80 0b [0a 04 00 7f 00 07 01 01 04 01 05] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
|| '83-L83-Key Reference' (für das Public Key-Objekt)

2.277.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.277.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_EXTERNAL_AUTHENTICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.278 Testfall: MSE SET mit CERT AT für externe Authentisierung (TC_MSE_SET_CERT_AT_EXTERNAL_AUTHENTICATION_FF_4)

2.278.1 Informationen

ID	TC_MSE_SET_CERT_AT_EXTERNAL_AUTHENTICATION_FF_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CERT AT für externe Authentisierung nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Dazu wird eine Kommandonachricht für MSE SET mit CERT AT für externe Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.278.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.278.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 80)

2.278.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_4						
CLA	INS	P1	P2	Lc	Data	Le

00	22	81	a4	LL	80 0b [0a 04 00 7f 00 07 01 01 04 01 03] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
|| '83-L83-Key Reference' (für das Public Key-Objekt)

2.278.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.278.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_EXTERNAL_AUTHENTICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.279 Testfall: MSE SET mit CERT AT für externe Authentisierung (TC_MSE_SET_CERT_AT_EXTERNAL_AUTHENTICATION_FF_5)

2.279.1 Informationen

ID	TC_MSE_SET_CERT_AT_EXTERNAL_AUTHENTICATION_FF_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CERT AT für externe Authentisierung nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Dazu wird eine Kommandonachricht für MSE SET mit CERT AT für externe Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.279.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.279.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_DEACTIVATED-1	Key-Objekt befindet sich im Zustand "operational state - deactivated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 80)

2.279.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_5						
CLA	INS	P1	P2	Lc	Data	Le

00	22	81	a4	LL	80 0b [0a 04 00 7f 00 07 01 01 04 01 03] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
|| '83-L83-Key Reference' (für das Public Key-Objekt)

2.279.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.279.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_EXTERNAL_AUTHENTICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.280 Testfall: MSE SET mit CRT AT für externe Authentisierung (TC_MSE_SET_CERT_AT_EXTERNAL_AUTHENTICATION_FF_6_1)

2.280.1 Informationen

ID	TC_MSE_SET_CERT_AT_EXTERNAL_AUTHENTICATION_FF_6_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für externe Authentisierung nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 80. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für externe Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.280.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.280.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 80)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.280.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_6_1						
CLA	INS	P1	P2	Lc	Data	Le

00	22	81	a4	LL	80 0b [ff 04 00 7f 00 07 01 01 04 01 03] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
|| '83-L83-Key Reference' (für das Public Key-Objekt)

2.280.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.280.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_EXTERNAL_AUTHENTICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.281 Testfall: MSE SET mit CERT AT für externe Authentisierung (TC_MSE_SET_CERT_AT_EXTERNAL_AUTHENTICATION_FF_6_2)

2.281.1 Informationen

ID	TC_MSE_SET_CERT_AT_EXTERNAL_AUTHENTICATION_FF_6_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CERT AT für externe Authentisierung nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 83. Dazu wird eine Kommandonachricht für MSE SET mit CERT AT für externe Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.281.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.281.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 83)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.281.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_6_2						
CLA	INS	P1	P2	Lc	Data	Le

00	22	81	a4	LL	80 0b [0a 04 00 7f 00 07 01 01 04 01 03] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
|| '83-L83-Key Reference' (für das Public Key-Objekt)

2.281.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.281.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.282 Testfall: MSE SET mit CRT AT für externe Authentisierung (TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_6_3)

2.282.1 Informationen

ID	TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_6_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für externe Authentisierung nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 80 fehlt. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für externe Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.282.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.282.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (80-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.282.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_6_3						
CLA	INS	P1	P2	Lc	Data	Le

00	22	81	a4	LL	83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)

|| '83-L83-Key Reference' (für das Public Key-Objekt)

2.282.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.282.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.283 Testfall: MSE SET mit CRT AT für externe Authentisierung (TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_6_4)

2.283.1 Informationen

ID	TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_6_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für externe Authentisierung nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 83 fehlt. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für externe Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.283.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.283.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (83-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.283.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_6_4							
CLA	INS	P1	P2	Lc	Data	Le	

00	22	81	a4	LL	80 0b [0a 04 00 7f 00 07 01 01 04 01 03]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)

|| '83-L83-Key Reference' (für das Public Key-Objekt)

2.283.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.283.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.284 Testfall: MSE SET mit CRT AT für externe Authentisierung (TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_6_5)

2.284.1 Informationen

ID	TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_6_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für externe Authentisierung nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 80 leer ist. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für externe Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.284.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.284.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (80-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.284.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_6_5							
CLA	INS	P1	P2	Lc	Data	Le	

00	22	81	a4	LL	80 00 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)

|| '83-L83-Key Reference' (für das Public Key-Objekt)

2.284.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.284.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.285 Testfall: MSE SET mit CRT AT für externe Authentisierung (TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_6_6)

2.285.1 Informationen

ID	TC_MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_6_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für externe Authentisierung nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 83 leer ist. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für externe Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.285.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_02

2.285.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (83-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.285.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_EXTERNAL_AUTHENTICATION_FF_6_6						
CLA	INS	P1	P2	Lc	Data	Le

00	22	81	a4	LL	800b [0a 04 00 7f 00 07 01 01 04 01 03] 83 00	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.285.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.285.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_EXTERNAL_AUTHENTICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.286 Testfall: MSE SET mit CRT AT für interne Authentisierung (TC_MSE_SET_CERT_AT_INTERNAL_AUTHENTICATION_GF_1)

2.286.1 Informationen

ID	TC_MSE_SET_CERT_AT_INTERNAL_AUTHENTICATION_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für interne Authentisierung erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für interne Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.286.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_03, VI_02_10

2.286.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.286.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_GF_1						
CLA	INS	P1	P2	Lc	Data	Le

00	22	41	a4	0f	80 0a [09 04 00 7f 00 07 01 01 04 01] 84 01 [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
|| '84-01-Key Reference' (für das Key Pair-Objekt)

2.286.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.286.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION-1	Nachfolgende Krypto-Operationen können ohne MSE-SET-bezogene Fehler erfolgreich ausgeführt werden.

2.287 Testfall: MSE SET mit CRT AT für interne Authentisierung (TC_MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_1)

2.287.1 Informationen

ID	TC_MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für interne Authentisierung nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für interne Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.287.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_03, VI_02_10

2.287.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.287.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_1						
CLA	INS	P1	P2	Lc	Data	Le

00	22	41	a4	0f	80 0a [09 04 00 7f 00 07 01 01 04 01] 84 01 [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
|| '84-01-Key Reference' (für das Key Pair-Objekt)

2.287.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.287.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.288 Testfall: MSE SET mit CRT AT für interne Authentisierung (TC_MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_2)

2.288.1 Informationen

ID	TC_MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für interne Authentisierung nicht erfolgreich durchgeführt werden kann, wenn das KEY-Objekt nicht gefunden wird. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für interne Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.288.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_03, VI_02_10

2.288.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	KEY-Objekt kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.288.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_2						
CLA	INS	P1	P2	Lc	Data	Le

00	22	41	a4	0f	80 0a [09 04 00 7f 00 07 01 01 04 01] 84 01 [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
|| '84-01-Key Reference' (für das Key Pair-Objekt)

2.288.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.288.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.289 Testfall: MSE SET mit CRT AT für interne Authentisierung (TC_MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_3)

2.289.1 Informationen

ID	TC_MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für interne Authentisierung nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für ECDSA ohne Hashing. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für interne Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.289.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_03, VI_02_10

2.289.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.289.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_3						
CLA	INS	P1	P2	Lc	Data	Le

00	22	41	a4	0f	80 0a [09 04 00 7f 00 07 01 01 04 01] 84 01 [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '84-01-Key Reference' (für das Key Pair-Objekt)

2.289.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.289.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_INTERNAL_AUTHENTICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.290 Testfall: MSE SET mit CRT AT für interne Authentisierung (TC_MSE_SET_CERT_AT_INTERNAL_AUTHENTICATION_FF_4)

2.290.1 Informationen

ID	TC_MSE_SET_CERT_AT_INTERNAL_AUTHENTICATION_FF_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für interne Authentisierung nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für interne Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.290.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_03, VI_02_10

2.290.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.290.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_4						
CLA	INS	P1	P2	Lc	Data	Le

00	22	41	a4	0f	80 0a [09 04 00 7f 00 07 01 01 04 01] 84 01 [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
|| '84-01-Key Reference' (für das Key Pair-Objekt)

2.290.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.290.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_INTERNAL_AUTHENTICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.291 Testfall: MSE SET mit CERT AT für interne Authentisierung (TC_MSE_SET_CERT_AT_INTERNAL_AUTHENTICATION_FF_5)

2.291.1 Informationen

ID	TC_MSE_SET_CERT_AT_INTERNAL_AUTHENTICATION_FF_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CERT AT für interne Authentisierung nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Dazu wird eine Kommandonachricht für MSE SET mit CERT AT für interne Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.291.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_03, VI_02_10

2.291.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_DEACTIVATED-1	Key-Objekt befindet sich im Zustand "operational state - deactivated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.291.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_5						
CLA	INS	P1	P2	Lc	Data	Le

00	22	41	a4	0f	80 0a [09 04 00 7f 00 07 01 01 04 01] 84 01 [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
|| '84-01-Key Reference' (für das Key Pair-Objekt)

2.291.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.291.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_INTERNAL_AUTHENTICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.292 Testfall: MSE SET mit CRT AT für interne Authentisierung (TC_MSE_SET_CERT_AT_INTERNAL_AUTHENTICATION_FF_6_1)

2.292.1 Informationen

ID	TC_MSE_SET_CERT_AT_INTERNAL_AUTHENTICATION_FF_6_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für interne Authentisierung nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 80 fehlt. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für interne Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.292.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_03, VI_02_10

2.292.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (80-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.292.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_6_1						
CLA	INS	P1	P2	Lc	Data	Le

00	22	41	a4	03	84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)

|| '84-01-Key Reference' (für das Key Pair-Objekt)

2.292.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.292.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_INTERNAL_AUTHENTICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.293 Testfall: MSE SET mit CRT AT für interne Authentisierung (TC_MSE_SET_CERT_AT_INTERNAL_AUTHENTICATION_FF_6_2)

2.293.1 Informationen

ID	TC_MSE_SET_CERT_AT_INTERNAL_AUTHENTICATION_FF_6_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für interne Authentisierung nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 80 leer ist. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für interne Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.293.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_03, VI_02_10

2.293.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (80-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.293.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_6_2						
CLA	INS	P1	P2	Lc	Data	Le

00	22	41	a4	05	80 00 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)

|| '84-01-Key Reference' (für das Key Pair-Objekt)

2.293.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.293.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.294 Testfall: MSE SET mit CRT AT für interne Authentisierung (TC_MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_6_3)

2.294.1 Informationen

ID	TC_MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_6_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für interne Authentisierung nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 84 fehlt. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für interne Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.294.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_03, VI_02_10

2.294.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (84-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.294.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_6_3						
CLA	INS	P1	P2	Lc	Data	Le

00	22	41	a4	0c	80 0a [09 04 00 7f 00 07 01 01 04 01]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)

|| '84-01-Key Reference' (für das Key Pair-Objekt)

2.294.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.294.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.295 Testfall: MSE SET mit CRT AT für interne Authentisierung (TC_MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_6_4)

2.295.1 Informationen

ID	TC_MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_6_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für interne Authentisierung nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 84 leer ist. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für interne Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.295.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_03, VI_02_10

2.295.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (84-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.295.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_6_4						
CLA	INS	P1	P2	Lc	Data	Le

00	22	41	a4	0e	80 0a [09 04 00 7f 00 07 01 01 04 01] 84 00	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)

|| '84-01-Key Reference' (für das Key Pair-Objekt)

2.295.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.295.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.296 Testfall: MSE SET mit CRT AT für interne Authentisierung (TC_MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_6_5)

2.296.1 Informationen

ID	TC_MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_6_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für interne Authentisierung nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 80. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für interne Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.296.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_03, VI_02_10

2.296.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 80)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.296.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_6_5						
CLA	INS	P1	P2	Lc	Data	Le

00	22	41	a4	0f	80 0a [ff 04 00 7f 00 07 01 01 04 01] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '84-01-Key Reference' (für das Key Pair-Objekt)

2.296.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.296.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_INTERNAL_AUTHENTICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.297 Testfall: MSE SET mit CRT AT für interne Authentisierung (TC_MSE_SET_CERT_AT_INTERNAL_AUTHENTICATION_FF_6_6)

2.297.1 Informationen

ID	TC_MSE_SET_CERT_AT_INTERNAL_AUTHENTICATION_FF_6_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für interne Authentisierung nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 84. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für interne Authentisierung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.297.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_03, VI_02_10

2.297.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 84)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.297.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION_FF_6_6						
CLA	INS	P1	P2	Lc	Data	Le

00	22	41	a4	0f	80 0a [09 04 00 7f 00 07 01 01 04 01] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '84-01-Key Reference' (für das Key Pair-Objekt)

2.297.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.297.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_INTERNAL_AUTHENTICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.298 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_GF_1_1)

2.298.1 Informationen

ID	TC_MSE_SET_CRT_AT_KEY_AGREEMENT_GF_1_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Die Durchführung erfolgt für ECKA-EG mit dem SM als Empfänger. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.298.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.298.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.298.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_GF_1_1						
CLA	INS	P1	P2	Lc	Data	Le

00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.298.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.298.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_KEY_AGREEMENT-1	Nachfolgende Krypto-Operationen können ohne MSE-SET-bezogene Fehler erfolgreich ausgeführt werden.

2.299 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_GF_1_2)

2.299.1 Informationen

ID	TC_MSE_SET_CRT_AT_KEY_AGREEMENT_GF_1_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement erfolgreich durchgeführt werden kann, sofern alle

	notwendigen Voraussetzungen erfüllt sind. Die Durchführung erfolgt für ECKA-EG mit dem SM als Initiator. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.299.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.299.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

CN- INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.299.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_GF_1_2						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.299.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.299.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_KEY_AGREEMENT-1	Nachfolgende Krypto-Operationen können ohne MSE-SET-bezogene Fehler erfolgreich ausgeführt werden.

2.300 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_GF_1_3)

2.300.1 Informationen

ID	TC_MSE_SET_CRT_AT_KEY_AGREEMENT_GF_1_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Die Durchführung erfolgt für ECKA-DH mit dem SM als Client. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.300.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.300.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FU	Schlüssel unterstützt Algorithmus

NCTION-2	
CN-SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.300.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_GF_1_3						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.300.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.300.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_KEY_AGREEMENT-1	Nachfolgende Krypto-Operationen können ohne MSE-SET-bezogene Fehler erfolgreich ausgeführt werden.

2.301 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CERT_AT_KEY_AGREEMENT_GF_1_4)

2.301.1 Informationen

ID	TC_MSE_SET_CERT_AT_KEY_AGREEMENT_GF_1_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Die Durchführung erfolgt für ECKA-DH mit dem SM als Server. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.301.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.301.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

INSTRUCTION_NOT_SUPPORTED-2	
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.301.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_GF_1_4						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder

Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.301.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.301.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_KEY_AGREEMENT-1	Nachfolgende Krypto-Operationen können ohne MSE-SET-bezogene Fehler erfolgreich ausgeführt werden.

2.302 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_1)

2.302.1 Informationen

ID	TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.302.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.302.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.302.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten

sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.302.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.302.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.303 Testfall: MSE SET mit CERT AT für Key-Agreement (TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_2_1)

2.303.1 Informationen

ID	TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_2_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CERT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn das KEY-Objekt nicht gefunden wird. Die Durchführung erfolgt für ECKA-EG mit dem SM als Initiator. Dazu wird eine Kommandonachricht für MSE SET mit CERT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.303.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.303.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	KEY-Objekt kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.303.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_2_1						
CLA	INS	P1	P2	Lc	Data	Le

00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.303.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.303.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.304 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_2_2)

2.304.1 Informationen

ID	TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_2_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn das

	KEY-Objekt nicht gefunden wird. Die Durchführung erfolgt für ECKA-EG mit dem SM als Empfänger. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.304.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.304.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	KEY-Objekt kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

CN- INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.304.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_2_2						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.304.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.304.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.305 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_2_3)

2.305.1 Informationen

ID	TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_2_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn das KEY-Objekt nicht gefunden wird. Die Durchführung erfolgt für ECKA-DH mit dem SM als Client. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.305.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.305.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	KEY-Objekt kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-UNSUPPORTED_FU	Schlüssel unterstützt Algorithmus

NCTION-2	
CN-SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.305.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_2_3						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.305.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.305.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.306 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_2_4)

2.306.1 Informationen

ID	TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_2_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn das KEY-Objekt nicht gefunden wird. Die Durchführung erfolgt für ECKA-DH mit dem SM als Server. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.306.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.306.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-	KEY-Objekt kann nicht gefunden werden

KEY_NOT_FOUND-1	
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.306.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_2_4						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder

Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.306.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.306.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.307 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_3_1)

2.307.1 Informationen

ID	TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_3_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für ECKA-EG mit dem SM als Initiator. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.307.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.307.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.307.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_3_1						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten

sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.307.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.307.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.308 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_3_2)

2.308.1 Informationen

ID	TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_3_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für ECKA-EG mit dem SM als Empfänger. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.

Klassifizierung	Fehlerfall-Test

2.308.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.308.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.308.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_3_2						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.308.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.308.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.309 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_3_3)

2.309.1 Informationen

ID	TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_3_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für ECKA-DH mit dem SM als Client. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.309.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.309.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-	KEY-Objekt kann gefunden werden

2	
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN- OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.309.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_3_3						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.309.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.309.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.310 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_3_4)

2.310.1 Informationen

ID	TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_3_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für ECKA-DH mit dem SM als Server. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.310.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.310.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-	Schlüssel unterstützt Algorithmus nicht

UNSUPPORTED_FUNCTION-1	
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.310.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_3_4						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder

Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.310.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.310.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.311 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_4_1)

2.311.1 Informationen

ID	TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_4_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Die Durchführung erfolgt für ECKA-EG mit dem SM als Initiator. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.311.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.311.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.311.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_4_1						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten

sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.311.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.311.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.312 Testfall: MSE SET mit CERT AT für Key-Agreement (TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_4_2)

2.312.1 Informationen

ID	TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_4_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CERT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Die Durchführung erfolgt für ECKA-EG mit dem SM als Empfänger. Dazu wird eine Kommandonachricht für MSE SET mit CERT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.

Klassifizierung	Fehlerfall-Test

2.312.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.312.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.312.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_4_2						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.312.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.312.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.313 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_4_3)

2.313.1 Informationen

ID	TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_4_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Die Durchführung erfolgt für ECKA-DH mit dem SM als Client. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.313.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.313.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.313.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_4_3						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.313.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.313.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.314 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_4_4)

2.314.1 Informationen

ID	TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_4_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Die Durchführung erfolgt für ECKA-DH mit dem SM als Server. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.314.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.314.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN- SECURITY_STATU S_NOT_SATISFIED- 1	Zugriffsregel ist nicht erfüllt
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- KEY_NOT_FOUND- 2	KEY-Objekt kann gefunden werden
CN- UNSUPPORTED_FU NCTION-2	Schlüssel unterstützt Algorithmus
CN- OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.314.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_4_4						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder

Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.314.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.314.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.315 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_5_1)

2.315.1 Informationen

ID	TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_5_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Die Durchführung erfolgt für ECKA-EG mit dem SM als Initiator. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.315.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.315.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_DEACTIVATED-1	Key-Objekt befindet sich im Zustand "operational state - deactivated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.315.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_5_1						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten

sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.315.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.315.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.316 Testfall: MSE SET mit CERT AT für Key-Agreement (TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_5_2)

2.316.1 Informationen

ID	TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_5_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CERT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Die Durchführung erfolgt für ECKA-EG mit dem SM als Empfänger. Dazu wird eine Kommandonachricht für MSE SET mit CERT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.

Klassifizierung	Fehlerfall-Test

2.316.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.316.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_DEACTIVATED-1	Key-Objekt befindet sich im Zustand "operational state - deactivated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.316.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_5_2						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.316.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.316.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.317 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_5_3)

2.317.1 Informationen

ID	TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_5_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Die Durchführung erfolgt für ECKA-DH mit dem SM als Client. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.317.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.317.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_DEACTIVATED-1	Key-Objekt befindet sich im Zustand "operational state - deactivated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-	KEY-Objekt kann gefunden werden

KEY_NOT_FOUND-2	
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.317.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_5_3						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.317.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.317.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.318 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_5_4)

2.318.1 Informationen

ID	TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_5_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Die Durchführung erfolgt für ECKA-DH mit dem SM als Server. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.318.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.318.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN- OBJECT_DEACTIVATED-1	Key-Objekt befindet sich im Zustand "operational state - deactivated"
CN- INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN- UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN- SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN- INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.318.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_5_4						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder

Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.318.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.318.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.319 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_6_1)

2.319.1 Informationen

ID	TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_6_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 80 fehlt. Die Durchführung erfolgt für ECKA-EG mit dem SM als Empfänger. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.319.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.319.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (80-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.319.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_1						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit

SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.319.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.319.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.320 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_6_2)

2.320.1 Informationen

ID	TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_6_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 84 fehlt. Die Durchführung erfolgt für ECKA-EG mit dem SM als Empfänger. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.

Klassifizierung	Fehlerfall-Test

2.320.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.320.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (84-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.320.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_2						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.320.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.320.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.321 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_3)

2.321.1 Informationen

ID	TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 80 leer ist. Die Durchführung erfolgt für ECKA-EG mit dem SM als Empfänger. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.321.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.321.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (80-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.321.4 APDU-Kommandos

ID: CM-MSE_SET_CERT_AT_KEY_AGREEMENT_FF_6_3						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 00 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.321.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.321.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.322 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_4)

2.322.1 Informationen

ID	TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 84 leer ist. Die Durchführung erfolgt für ECKA-EG mit dem SM als Empfänger. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.322.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.322.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN- INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (84-Objekt ist leer)
CN- INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN- UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN- SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN- OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.322.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_4						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 00	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder

Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.322.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.322.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.323 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_6_5)

2.323.1 Informationen

ID	TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_6_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 80. Die Durchführung erfolgt für ECKA-EG mit dem SM als Empfänger. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.323.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.323.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 80)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.323.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_5						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten

sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.323.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.323.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.324 Testfall: MSE SET mit CERT AT für Key-Agreement (TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_6_6)

2.324.1 Informationen

ID	TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_6_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CERT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 84. Die Durchführung erfolgt für ECKA-EG mit dem SM als Empfänger. Dazu wird eine Kommandonachricht für MSE SET mit CERT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.

Klassifizierung	Fehlerfall-Test

2.324.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.324.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 84)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.324.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_6						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.324.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.324.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.325 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_7)

2.325.1 Informationen

ID	TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_7
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 80 fehlt. Die Durchführung erfolgt für ECKA-EG mit dem SM als Initiator. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.325.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.325.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (80-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-	KEY-Objekt kann gefunden werden

KEY_NOT_FOUND-2	
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.325.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_7						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	83 LL [XX...XX] 84 01 [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.325.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.325.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.326 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_6_8)

2.326.1 Informationen

ID	TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_6_8
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 83 fehlt. Die Durchführung erfolgt für ECKA-EG mit dem SM als Initiator. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.326.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.326.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN- INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (83-Objekt fehlt)
CN- INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN- UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN- SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN- OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.326.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_8						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder

Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.326.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.326.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.327 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_6_9)

2.327.1 Informationen

ID	TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_6_9
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 80 leer ist. Die Durchführung erfolgt für ECKA-EG mit dem SM als Initiator. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.327.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.327.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (80-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.327.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_9						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 00 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit

SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.327.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.327.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.328 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_6_10)

2.328.1 Informationen

ID	TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_6_10
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 83 leer ist. Die Durchführung erfolgt für ECKA-EG mit dem SM als Initiator. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.

Klassifizierung	Fehlerfall-Test

2.328.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.328.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (83-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.328.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_10						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 00 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.328.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.328.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.329 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_11)

2.329.1 Informationen

ID	TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_11
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 80. Die Durchführung erfolgt für ECKA-EG mit dem SM als Initiator. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.329.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.329.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 80)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-	KEY-Objekt kann gefunden werden

KEY_NOT_FOUND-2	
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.329.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_11						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.329.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.329.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.330 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_12)

2.330.1 Informationen

ID	TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_12
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 83. Die Durchführung erfolgt für ECKA-EG mit dem SM als Initiator. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.330.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.330.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN- INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 83)
CN- INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN- UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN- SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN- OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.330.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_12						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder

Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.330.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.330.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.331 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_13)

2.331.1 Informationen

ID	TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_13
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 80. Die Durchführung erfolgt für ECKA-DH mit dem SM als Initiator. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.331.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.331.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 80)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.331.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_13						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten

sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.331.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.331.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.332 Testfall: MSE SET mit CERT AT für Key-Agreement (TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_6_14)

2.332.1 Informationen

ID	TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_6_14
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CERT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 80. Die Durchführung erfolgt für ECKA-DH mit dem SM als Empfänger. Dazu wird eine Kommandonachricht für MSE SET mit CERT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.

Klassifizierung	Fehlerfall-Test

2.332.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.332.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 80)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.332.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_14						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.332.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.332.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.333 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_15)

2.333.1 Informationen

ID	TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_15
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 80 fehlt. Die Durchführung erfolgt für ECKA-DH mit dem SM als Initiator. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.333.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.333.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (80-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-	KEY-Objekt kann gefunden werden

KEY_NOT_FOUND-2	
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.333.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_15						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.333.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.333.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.334 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_16)

2.334.1 Informationen

ID	TC_MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_16
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 80 fehlt. Die Durchführung erfolgt für ECKA-DH mit dem SM als Empfänger. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.334.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.334.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (80-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.334.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_16						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder

Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.334.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.334.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.335 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_6_17)

2.335.1 Informationen

ID	TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_6_17
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 80 leer ist. Die Durchführung erfolgt für ECKA-DH mit dem SM als Initiator. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.335.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.335.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (80-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.335.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_17						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 00 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit

SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.335.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.335.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CERT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.336 Testfall: MSE SET mit CRT AT für Key-Agreement (TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_6_18)

2.336.1 Informationen

ID	TC_MSE_SET_CERT_AT_KEY_AGREEMENT_FF_6_18
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für Key-Agreement nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 80 leer ist. Die Durchführung erfolgt für ECKA-DH mit dem SM als Empfänger. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für Key-Agreement zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.

Klassifizierung	Fehlerfall-Test

2.336.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_05, PN_05_06, PN_05_07, PN_05_08a, PN_05_08b

2.336.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (80-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.336.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_KEY_AGREEMENT_FF_6_18						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 00 83 LL [XX...XX] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

2.336.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.336.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_KEY_AGREEMENT-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.337 Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_GF_1)

2.337.1 Informationen

ID	TC_MSE_SET_CRT_AT_PACE_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für PACE erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für PACE zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.337.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.337.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- PASSWORD_NOT_ FOUND-2	Das PIN-Objekt kann gefunden werden
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

CN- INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.337.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_PACE_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 01 [XX...XX] 84 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID PACE-Protokoll' (nur Wert ohne Tag '06') || '83-01-PIN Reference' für das PIN-Objekt || '84-L84-ID der Ellipt. Kurve' (notwendig, da mehrere Ellipt. Kurven für das PACE-Protokoll möglich sind; ID gemäß [TR-03110-3])

2.337.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.337.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_PACE-1	Nachfolgende Krypto-Operationen können ohne MSE-SET-bezogene Folgefehler erfolgreich ausgeführt werden.

2.338 Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_FF_1)

2.338.1 Informationen

ID	TC_MSE_SET_CRT_AT_PACE_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für PACE nicht erfolgreich durchgeführt werden kann, wenn sich das

	Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für PACE zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.338.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.338.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-PASSWORD_NOT_FOUND-2	Das PIN-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.338.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_PACE_FF_1						
CLA	INS	P1	P2	Lc	Data	Le

00	22	c1	a4	LL	80 LL [XX...XX] 83 01 [XX...XX] 84 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID PACE-Protokoll' (nur Wert ohne Tag '06') || '83-01-PIN Reference' für das PIN-Objekt || '84-L84-ID der Ellipt. Kurve' (notwendig, da mehrere Ellipt. Kurven für das PACE-Protokoll möglich sind; ID gemäß [TR-03110-3])

2.338.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.338.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_PACE-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Folgefehler ausgeführt werden.

2.339 Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_FF_2)

2.339.1 Informationen

ID	TC_MSE_SET_CRT_AT_PACE_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für PACE nicht erfolgreich durchgeführt werden kann, wenn das mittels P2-Parameter adressierte PIN-Objekt nicht gefunden wird. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für PACE zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.339.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.339.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-PASSWORD_NOT_FOUND-1	Das PIN-Objekt kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.339.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_PACE_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 01 [XX...XX] 84 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID PACE-Protokoll' (nur Wert ohne Tag '06') || '83-01-PIN Reference' für das PIN-Objekt || '84-L84-ID der Ellipt. Kurve' (notwendig, da mehrere Ellipt. Kurven für das PACE-Protokoll möglich sind; ID gemäß [TR-03110-3])

2.339.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.339.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_PACE-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Folgefehler ausgeführt werden.

2.340 Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_FF_3)

2.340.1 Informationen

ID	TC_MSE_SET_CRT_AT_PACE_FF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für PACE nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für PACE zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.340.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.340.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- SECURITY_STATU S_NOT_SATISFIED- 1	Zugriffsregel ist nicht erfüllt
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- PASSWORD_NOT_ FOUND-2	Das PIN-Objekt kann gefunden werden
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt fehlt nicht)

2.340.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_PACE_FF_3						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 01 [XX...XX] 84 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID PACE-Protokoll' (nur Wert ohne Tag '06') || '83-01-PIN Reference' für das PIN-Objekt || '84-L84-ID der Ellipt. Kurve' (notwendig, da mehrere Ellipt. Kurven für das PACE-Protokoll möglich sind; ID gemäß [TR-03110-3])

2.340.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.340.6 Verifikationen

ID	Beschreibung

VF-MSE_SET_CRT_AT_PACE-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Folgefehler ausgeführt werden.

2.341 Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_FF_4_1)

2.341.1 Informationen

ID	TC_MSE_SET_CRT_AT_PACE_FF_4_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für PACE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 80 fehlt. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für PACE zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.341.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.341.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (80-Objekt fehlt)
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN-PASSWORD_NOT_FOUND-2	Das PIN-Objekt kann gefunden werden
CN-SECURITY_STATU S_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.341.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_PACE_FF_4_1						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	83 01 [XX] 84 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID PACE-Protokoll' (nur Wert ohne Tag '06') || '83-01-PIN Reference' für das PIN-Objekt || '84-L84-ID der Ellipt. Kurve' (notwendig, da mehrere Ellipt. Kurven für das PACE-Protokoll möglich sind; ID gemäß [TR-03110-3])

2.341.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.341.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_PACE-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Folgefehler ausgeführt werden.

2.342 Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_FF_4_2)

2.342.1 Informationen

ID	TC_MSE_SET_CRT_AT_PACE_FF_4_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für PACE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 80 leer ist. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für PACE zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.342.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.342.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (80-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PASSWORD_NOT_FOUND-2	Das PIN-Objekt kann gefunden werden

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.342.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_PACE_FF_4_2						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 00 83 01 [XX] 84 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID PACE-Protokoll' (nur Wert ohne Tag '06') || '83-01-PIN Reference' für das PIN-Objekt || '84-L84-ID der Ellipt. Kurve' (notwendig, da mehrere Ellipt. Kurven für das PACE-Protokoll möglich sind; ID gemäß [TR-03110-3])

2.342.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.342.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_PACE-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Folgefehler ausgeführt werden.

2.343 Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_FF_4_3)

2.343.1 Informationen

ID	TC_MSE_SET_CRT_AT_PACE_FF_4_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für PACE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im

	Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 83 fehlt. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für PACE zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.343.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.343.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (83-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PASSWORD_NOT_FOUND-2	Das PIN-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.343.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_PACE_FF_4_3

CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 84 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID PACE-Protokoll' (nur Wert ohne Tag '06') || '83-01-PIN Reference' für das PIN-Objekt || '84-L84-ID der Ellipt. Kurve' (notwendig, da mehrere Ellipt. Kurven für das PACE-Protokoll möglich sind; ID gemäß [TR-03110-3])

2.343.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.343.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_PACE-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Folgefehler ausgeführt werden.

2.344 Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_FF_4_4)

2.344.1 Informationen

ID	TC_MSE_SET_CRT_AT_PACE_FF_4_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für PACE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 83 leer ist. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für PACE zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.344.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.344.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (83-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PASSWORD_NOT_FOUND-2	Das PIN-Objekt kann gefunden werden
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.344.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_PACE_FF_4_4						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 00 84 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID PACE-Protokoll' (nur Wert ohne Tag '06') || '83-01-PIN Reference' für das PIN-Objekt || '84-L84-ID der Ellipt. Kurve' (notwendig, da mehrere Ellipt. Kurven für das PACE-Protokoll möglich sind; ID gemäß [TR-03110-3])

2.344.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.344.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_PACE-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Folgefehler ausgeführt werden.

2.345 Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_FF_4_5)

2.345.1 Informationen

ID	TC_MSE_SET_CRT_AT_PACE_FF_4_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für PACE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 84 fehlt. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für PACE zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.345.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.345.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (84-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PASSWORD_NOT_FOUND-2	Das PIN-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.345.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_PACE_FF_4_5						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 01 [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID PACE-Protokoll' (nur Wert ohne Tag '06') || '83-01-PIN Reference' für das PIN-Objekt || '84-L84-ID der Ellipt. Kurve' (notwendig, da mehrere Ellipt. Kurven für das PACE-Protokoll möglich sind; ID gemäß [TR-03110-3])

2.345.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.345.6 Verifikationen

ID	Beschreibung

VF-MSE_SET_CRT_AT_PACE-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Folgefehler ausgeführt werden.

2.346 Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_FF_4_6)

2.346.1 Informationen

ID	TC_MSE_SET_CRT_AT_PACE_FF_4_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für PACE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 84 leer ist. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für PACE zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.346.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.346.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (84-Objekt ist leer)
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN-PASSWORD_NOT_FOUND-2	Das PIN-Objekt kann gefunden werden
CN-SECURITY_STATU S_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.346.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_PACE_FF_4_6						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 01 [XX] 84 00	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID PACE-Protokoll' (nur Wert ohne Tag '06') || '83-01-PIN Reference' für das PIN-Objekt || '84-L84-ID der Ellipt. Kurve' (notwendig, da mehrere Ellipt. Kurven für das PACE-Protokoll möglich sind; ID gemäß [TR-03110-3])

2.346.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.346.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_PACE-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Folgefehler ausgeführt werden.

2.347 Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_FF_4_7)

2.347.1 Informationen

ID	TC_MSE_SET_CRT_AT_PACE_FF_4_7
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für PACE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 80. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für PACE zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.347.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.347.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 80)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PASSWORD_NOT_FOUND-2	Das PIN-Objekt kann gefunden werden

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.347.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_PACE_FF_4_7						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 01 [XX] 84 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID PACE-Protokoll' (nur Wert ohne Tag '06') || '83-01-PIN Reference' für das PIN-Objekt || '84-L84-ID der Ellipt. Kurve' (notwendig, da mehrere Ellipt. Kurven für das PACE-Protokoll möglich sind; ID gemäß [TR-03110-3])

2.347.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.347.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_PACE-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Folgefehler ausgeführt werden.

2.348 Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_FF_4_8)

2.348.1 Informationen

ID	TC_MSE_SET_CRT_AT_PACE_FF_4_8
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für

	PACE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 83. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für PACE zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.348.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.348.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 83)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PASSWORD_NOT_FOUND-2	Das PIN-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.348.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_PACE_FF_4_8

CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	LL	80 LL [XX...XX] 83 01 [XX] 84 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID PACE-Protokoll' (nur Wert ohne Tag '06') || '83-01-PIN Reference' für das PIN-Objekt || '84-L84-ID der Ellipt. Kurve' (notwendig, da mehrere Ellipt. Kurven für das PACE-Protokoll möglich sind; ID gemäß [TR-03110-3])

2.348.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.348.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_PACE-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Folgefehler ausgeführt werden.

2.349 Testfall: MSE SET mit CRT AT für PACE (TC_MSE_SET_CRT_AT_PACE_FF_4_9)

2.349.1 Informationen

ID	TC_MSE_SET_CRT_AT_PACE_FF_4_9
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT AT für PACE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 84. Dazu wird eine Kommandonachricht für MSE SET mit CRT AT für PACE zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.349.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_03_01

2.349.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 84)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PASSWORD_NOT_FOUND-2	Das PIN-Objekt kann gefunden werden
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.349.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_AT_PACE_FF_4_9							
CLA	INS	P1	P2	Lc	Data	Le	
00	22	c1	a4	LL	80 LL [XX...XX] 83 01 [XX] 84 LL [XX...XX]	--	

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID PACE-Protokoll' (nur Wert ohne Tag '06') || '83-01-PIN Reference' für das PIN-Objekt || '84-L84-ID der Ellipt. Kurve' (notwendig, da mehrere Ellipt. Kurven für das PACE-Protokoll möglich sind; ID gemäß [TR-03110-3])

2.349.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.349.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_AT_PACE-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Folgefehler ausgeführt werden.

2.350 Testfall: MSE SET mit CRT DST für Signaturerzeugung (TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_GF_1)

2.350.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signaturerzeugung erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signaturerzeugung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.350.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_09, PN_05_02

2.350.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt ist nicht leer)

2.350.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_GENERATION_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	22	41	b6	0f	80 0a [09 04 00 7f 00 07 01 01 04 01] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '84-01-Key Reference' (für das Key Pair-Objekt)

2.350.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.350.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_GENERATION-1	Nachfolgende Krypto-Operationen können ohne MSE-SET-bezogene Fehler erfolgreich ausgeführt werden.

2.351 Testfall: MSE SET mit CRT DST für Signaturerzeugung (TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_1)

2.351.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signaturerzeugung nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Die Durchführung erfolgt für ECDSA ohne Hashing. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signaturerzeugung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.351.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_09, PN_05_02

2.351.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt ist nicht leer)

2.351.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	22	41	b6	0f	80 0a [09 04 00 7f 00 07 01 01 04 01] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '84-01-Key Reference' (für das Key Pair-Objekt)

2.351.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.351.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_GENERATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.352 Testfall: MSE SET mit CRT DST für Signaturerzeugung (TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_2)

2.352.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signaturerzeugung nicht erfolgreich durchgeführt werden kann, wenn das KEY-Objekt nicht gefunden wird. Die Durchführung erfolgt für ECDSA ohne Hashing. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signaturerzeugung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.352.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_09, PN_05_02

2.352.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	KEY-Objekt kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt ist nicht leer)

2.352.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	22	41	b6	0f	80 0a [09 04 00 7f 00 07 01 01 04 01] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '84-01-Key Reference' (für das Key Pair-Objekt)

2.352.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.352.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_GENERATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.353 Testfall: MSE SET mit CRT DST für Signaturerzeugung (TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_3)

2.353.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signaturerzeugung nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für ECDSA ohne Hashing. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signaturerzeugung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.353.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_09, PN_05_02

2.353.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt ist nicht leer)

2.353.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_3						
CLA	INS	P1	P2	Lc	Data	Le
00	22	41	b6	0f	80 0a [09 04 00 7f 00 07 01 01 04 01] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '84-01-Key Reference' (für das Key Pair-Objekt)

2.353.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.353.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_GENERATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.354 Testfall: MSE SET mit CRT DST für Signaturerzeugung (TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_4)

2.354.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signaturerzeugung nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Die Durchführung erfolgt für ECDSA ohne Hashing. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signaturerzeugung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.354.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_09, PN_05_02

2.354.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt ist nicht leer)

2.354.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_4						
CLA	INS	P1	P2	Lc	Data	Le
00	22	41	b6	0f	80 0a [09 04 00 7f 00 07 01 01 04 01] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '84-01-Key Reference' (für das Key Pair-Objekt)

2.354.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.354.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_GENERATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.355 Testfall: MSE SET mit CRT DST für Signaturerzeugung (TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_5)

2.355.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signaturerzeugung nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Die Durchführung erfolgt für ECDSA ohne Hashing. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signaturerzeugung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.355.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_09, PN_05_02

2.355.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_DEACTIVATED-1	Key-Objekt befindet sich im Zustand "operational state - deactivated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (80-Objekt ist nicht leer)

2.355.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_5						
CLA	INS	P1	P2	Lc	Data	Le
00	22	41	b6	0f	80 0a [09 04 00 7f 00 07 01 01 04 01] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '84-01-Key Reference' (für das Key Pair-Objekt)

2.355.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.355.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_GENERATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.356 Testfall: MSE SET mit CRT DST für Signaturerzeugung (TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_6_1)

2.356.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_6_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signaturerzeugung nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 80 leer ist. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signaturerzeugung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.356.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_09, PN_05_02

2.356.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (80-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.356.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_6_1						
CLA	INS	P1	P2	Lc	Data	Le
00	22	41	b6	05	80 00 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '84-01-Key Reference' (für das Key Pair-Objekt)

2.356.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.356.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_GENERATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.357 Testfall: MSE SET mit CRT DST für Signaturerzeugung (TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_6_2)

2.357.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_6_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signaturerzeugung nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 84 leer ist. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signaturerzeugung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.357.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_09, PN_05_02

2.357.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (84-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.357.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_6_2						
CLA	INS	P1	P2	Lc	Data	Le
00	22	41	b6	0d	80 0a [09 04 00 7f 00 07 01 01 04 01] 84 00	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '84-01-Key Reference' (für das Key Pair-Objekt)

2.357.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.357.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_GENERATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.358 Testfall: MSE SET mit CRT DST für Signaturerzeugung (TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_6_3)

2.358.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_6_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signaturerzeugung nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 80 fehlt. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signaturerzeugung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.358.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_09, PN_05_02

2.358.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (80-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.358.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_6_3						
CLA	INS	P1	P2	Lc	Data	Le
00	22	41	b6	03	84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '84-01-Key Reference' (für das Key Pair-Objekt)

2.358.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.358.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_GENERATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.359 Testfall: MSE SET mit CRT DST für Signaturerzeugung (TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_6_4)

2.359.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_6_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signaturerzeugung nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 84 fehlt. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signaturerzeugung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.359.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_09, PN_05_02

2.359.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (84-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.359.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_6_4						
CLA	INS	P1	P2	Lc	Data	Le
00	22	41	b6	0c	80 0a [09 04 00 7f 00 07 01 01 04 01]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '84-01-Key Reference' (für das Key Pair-Objekt)

2.359.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.359.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_GENERATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.360 Testfall: MSE SET mit CRT DST für Signaturerzeugung (TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_6_5)

2.360.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_6_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signaturerzeugung nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 80. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signaturerzeugung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.360.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_09, PN_05_02

2.360.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 80)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.360.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_6_5						
CLA	INS	P1	P2	Lc	Data	Le
00	22	41	b6	0f	80 0a [ff 04 00 7f 00 07 01 01 04 01] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '84-01-Key Reference' (für das Key Pair-Objekt)

2.360.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.360.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_GENERATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.361 Testfall: MSE SET mit CRT DST für Signaturerzeugung (TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_6_6)

2.361.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_6_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signaturerzeugung nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 83. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signaturerzeugung zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.361.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_09, PN_05_02

2.361.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 83)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.361.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_GENERATION_FF_6_6						
CLA	INS	P1	P2	Lc	Data	Le
00	22	41	b6	0f	80 0a [09 04 00 7f 00 07 01 01 04 01] 84 01 [XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '84-01-Key Reference' (für das Key Pair-Objekt)

2.361.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.361.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_GENERATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.362 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_GF_1)

2.362.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.362.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.362.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt

2.362.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0a [09 04 00 7f 00 07 01 01 04 01] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.362.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.362.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-1	Nachfolgende Krypto-Operationen können ohne MSE-SET-bezogene Fehler erfolgreich ausgeführt werden.

2.363 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_1_1)

2.363.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_1_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Die Durchführung erfolgt für ECDSA ohne Hashing. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.363.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.363.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt

2.363.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_1_1						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0a [09 04 00 7f 00 07 01 01 04 01] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.363.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.363.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.364 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_1_2)

2.364.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_1_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Die Durchführung erfolgt für ECDSA mit SHSA256. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.364.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.364.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt

2.364.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_1_2						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0b [09 04 00 7f 00 07 01 01 04 01 03] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.364.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.364.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.365 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_1_3)

2.365.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_1_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Die Durchführung erfolgt für ECDSA mit SHA384. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.365.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.365.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt

2.365.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_1_3						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0b [09 04 00 7f 00 07 01 01 04 01 04] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.365.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.365.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.366 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_1_4)

2.366.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_1_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Die Durchführung erfolgt für ECDSA mit SHA512. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.366.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.366.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt

2.366.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_1_4						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0b [09 04 00 7f 00 07 01 01 04 01 05] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.366.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.366.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.367 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_2_1)

2.367.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_2_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation nicht erfolgreich durchgeführt werden kann, wenn das KEY-Objekt nicht gefunden wird. Die Durchführung erfolgt für ECDSA ohne Hashing. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.367.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.367.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	KEY-Objekt kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt

2.367.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_2_1						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0a [09 04 00 7f 00 07 01 01 04 01] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.367.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.367.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.368 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_2_2)

2.368.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_2_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation nicht erfolgreich durchgeführt werden kann, wenn das KEY-Objekt nicht gefunden wird. Die Durchführung erfolgt für ECDSA mit SHSA256. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.368.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.368.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	KEY-Objekt kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt

2.368.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_2_2						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0b [09 04 00 7f 00 07 01 01 04 01 03] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.368.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.368.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.369 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_2_3)

2.369.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_2_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation nicht erfolgreich durchgeführt werden kann, wenn das KEY-Objekt nicht gefunden wird. Die Durchführung erfolgt für ECDSA mit SHA384. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.369.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.369.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	KEY-Objekt kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt

2.369.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_2_3						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0b [09 04 00 7f 00 07 01 01 04 01 04] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.369.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.369.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.370 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_2_4)

2.370.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_2_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation nicht erfolgreich durchgeführt werden kann, wenn das KEY-Objekt nicht gefunden wird. Die Durchführung erfolgt für ECDSA mit SHA512. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.370.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.370.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	KEY-Objekt kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt

2.370.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_2_4						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0b [09 04 00 7f 00 07 01 01 04 01 05] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.370.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.370.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.371 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_3_1)

2.371.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_3_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für ECDSA ohne Hashing. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.371.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.371.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt

2.371.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_3_1						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0a [09 04 00 7f 00 07 01 01 04 01] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.371.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.371.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.372 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_3_2)

2.372.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_3_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für ECDSA mit SHA256. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.372.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.372.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt

2.372.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_3_2						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0b [09 04 00 7f 00 07 01 01 04 01 03] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.372.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.372.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.373 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_3_3)

2.373.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_3_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für ECDSA mit SHA384. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.373.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.373.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt

2.373.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_3_3						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0b [09 04 00 7f 00 07 01 01 04 01 04] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.373.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.373.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.374 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_3_4)

2.374.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_3_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für ECDSA mit SHA512. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.374.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.374.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt

2.374.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_3_4						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0b [09 04 00 7f 00 07 01 01 04 01 05] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.374.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.374.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.375 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_4_1)

2.375.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_4_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Die Durchführung erfolgt für ECDSA ohne Hashing. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.375.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.375.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt

2.375.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_4_1						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0a [09 04 00 7f 00 07 01 01 04 01] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.375.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.375.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.376 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_4_2)

2.376.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_4_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Die Durchführung erfolgt für ECDSA mit SHSA256. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.376.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.376.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt

2.376.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_4_2						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0b [09 04 00 7f 00 07 01 01 04 01 03] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.376.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.376.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.377 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_4_3)

2.377.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_4_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Die Durchführung erfolgt für ECDSA mit SHA384. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.377.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.377.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt

2.377.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_4_3						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0b [09 04 00 7f 00 07 01 01 04 01 04] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.377.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.377.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.378 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_4_4)

2.378.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_4_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Die Durchführung erfolgt für ECDSA mit SHA512. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.378.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.378.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt

2.378.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_4_4						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0b [09 04 00 7f 00 07 01 01 04 01 05] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.378.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.378.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.379 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_5_1)

2.379.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_5_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Die Durchführung erfolgt für ECDSA ohne Hashing. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.379.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.379.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_DEACTIVATED-1	Key-Objekt befindet sich im Zustand "operational state - deactivated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt

2.379.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_5_1						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0a [09 04 00 7f 00 07 01 01 04 01] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.379.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.379.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.380 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_5_2)

2.380.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_5_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Die Durchführung erfolgt für ECDSA mit SHA256. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.380.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.380.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_DEACTIVATED-1	Key-Objekt befindet sich im Zustand "operational state - deactivated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt

2.380.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_5_2						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0b [09 04 00 7f 00 07 01 01 04 01 03] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.380.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.380.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.381 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_5_3)

2.381.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_5_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Die Durchführung erfolgt für ECDSA mit SHA384. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.381.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.381.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_DEACTIVATED-1	Key-Objekt befindet sich im Zustand "operational state - deactivated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt

2.381.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_5_3						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0b [09 04 00 7f 00 07 01 01 04 01 04] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.381.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.381.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.382 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_5_4)

2.382.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_5_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Die Durchführung erfolgt für ECDSA mit SHA512. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.382.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.382.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_DEACTIVATED-1	Key-Objekt befindet sich im Zustand "operational state - deactivated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt

2.382.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_5_4						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0b [09 04 00 7f 00 07 01 01 04 01 05] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.382.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.382.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.383 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_6_1)

2.383.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_6_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt für ECDSA ohne Hashing. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.383.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.383.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.383.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_6_1						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0a [09 04 00 7f 00 07 01 01 04 01] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.383.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.383.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.384 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_6_2)

2.384.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_6_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt für ECDSA mit SHA256. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.384.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.384.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.384.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_6_2						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0b [09 04 00 7f 00 07 01 01 04 01 03] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.384.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.384.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.385 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_6_3)

2.385.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_6_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt für ECDSA mit SHA384. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.385.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.385.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.385.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_6_3						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0b [09 04 00 7f 00 07 01 01 04 01 04] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.385.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.385.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.386 Testfall: MSE SET mit CRT DST für Signatur- und Zertifikatverifikation (TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_6_4)

2.386.1 Informationen

ID	TC_MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_6_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando MSE SET mit CRT DST für Signatur- und Zertifikatverifikation nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt für ECDSA mit SHA512. Dazu wird eine Kommandonachricht für MSE SET mit CRT DST für Signatur- und Zertifikatverifikation zum Setzen von Parametern der SE an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.386.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.6.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_11, PN_05_04b, VI_02_07, VI_02_08, VI_02_11b

2.386.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.386.4 APDU-Kommandos

ID: CM-MSE_SET_CRT_DST_SIGNATURE_VERIFICATION_FF_6_4						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	LL	80 0b [09 04 00 7f 00 07 01 01 04 01 05] 83 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

2.386.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.386.6 Verifikationen

ID	Beschreibung
VF-MSE_SET_CRT_DST_VERIFICATION-2	Nachfolgende Krypto-Operationen können nicht ohne MSE-SET-bezogene Fehler ausgeführt werden.

2.387 Testfall: PSO COMPUTE DIGITAL SIGNATURE (TC_PSO_COMPUTE_DIGITAL_SIGNATURE_GF_1)

2.387.1 Informationen

ID	TC_PSO_COMPUTE_DIGITAL_SIGNATURE_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO COMPUTE DIGITAL SIGNATURE erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für PSO COMPUTE DIGITAL SIGNATURE zur Erzeugung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.387.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_02, VI_02_09

2.387.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.387.4 APDU-Kommandos

ID: CM-PSO_COMPUTE_DIGITAL_SIGNATURE_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.387.5 Erwartete Ergebnisse

ID	Beschreibung
RS-A766	XX XX 90 00

2.387.6 Verifikationen

ID	Beschreibung
VF- PSO_COMPUTE_DIGITAL_SIGNATURE-1	Die Signaturerstellung mit dem aus dem entsprechenden Key-Object ausgelesenen Prüfschlüssel stimmt mit der Signatur dieses Testfalls überein.

2.388 Testfall: PSO COMPUTE DIGITAL SIGNATURE (TC_PSO_COMPUTE_DIGITAL_SIGNATURE_FF_1)

2.388.1 Informationen

ID	TC_PSO_COMPUTE_DIGITAL_SIGNATURE_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO COMPUTE DIGITAL SIGNATURE nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für PSO COMPUTE DIGITAL SIGNATURE zur Erzeugung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.388.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_02, VI_02_09

2.388.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.388.4 APDU-Kommandos

ID: CM-PSO_COMPUTE_DIGITAL_SIGNATURE_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.388.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.388.6 Verifikationen

ID	Beschreibung
VF- PSO_COMPUTE_DIGITAL_SIGNATURE-2	Es wird keine Signatur zurückgegeben.

2.389 Testfall: PSO COMPUTE DIGITAL SIGNATURE (TC_PSO_COMPUTE_DIGITAL_SIGNATURE_FF_2)

2.389.1 Informationen

ID	TC_PSO_COMPUTE_DIGITAL_SIGNATURE_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO COMPUTE DIGITAL SIGNATURE nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt nicht ausgewählt ist. Dazu wird eine Kommandonachricht für PSO COMPUTE DIGITAL SIGNATURE zur Erzeugung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.389.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_02, VI_02_09

2.389.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft

SEMANTIC_CORRECTNESS	(soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-NO_KEY_REFERENCE-1	Key-Objekt ist nicht ausgewählt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.389.4 APDU-Kommandos

ID: CM-PSO_COMPUTE_DIGITAL_SIGNATURE_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.389.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6985	Das Testsystem antwortet mit '69 85'.

2.389.6 Verifikationen

ID	Beschreibung
VF- PSO_COMPUTE_DIGITAL_SIGNATURE-2	Es wird keine Signatur zurückgegeben.

2.390 Testfall: PSO COMPUTE DIGITAL SIGNATURE (TC_PSO_COMPUTE_DIGITAL_SIGNATURE_FF_3)

2.390.1 Informationen

ID	TC_PSO_COMPUTE_DIGITAL_SIGNATURE_FF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO COMPUTE DIGITAL SIGNATURE nicht erfolgreich durchgeführt werden kann, wenn das KEY-Objekt nicht gefunden wird. Dazu wird eine Kommandonachricht für PSO COMPUTE DIGITAL SIGNATURE zur Erzeugung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.390.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_02, VI_02_09

2.390.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-	KEY-Objekt kann nicht gefunden werden

KEY_NOT_FOUND-1	
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.390.4 APDU-Kommandos

ID: CM-PSO_COMPUTE_DIGITAL_SIGNATURE_FF_3						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.390.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.390.6 Verifikationen

ID	Beschreibung
VF- PSO_COMPUTE_DIGITAL_SIGNATURE-2	Es wird keine Signatur zurückgegeben.

2.391 Testfall: PSO COMPUTE DIGITAL SIGNATURE (TC_PSO_COMPUTE_DIGITAL_SIGNATURE_FF_4)

2.391.1 Informationen

ID	TC_PSO_COMPUTE_DIGITAL_SIGNATURE_FF_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO COMPUTE DIGITAL SIGNATURE nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Dazu wird eine Kommandonachricht für PSO COMPUTE DIGITAL SIGNATURE zur Erzeugung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.391.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_02, VI_02_09

2.391.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- SECURITY_STATU S_NOT_SATISFIED- 1	Zugriffsregel ist nicht erfüllt

CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.391.4 APDU-Kommandos

ID: CM-PSO_COMPUTE_DIGITAL_SIGNATURE_FF_4						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.391.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.391.6 Verifikationen

ID	Beschreibung

VF- PSO_COMPUTE_DIGITAL_SIGNATURE-2	Es wird keine Signatur zurückgegeben.

2.392 Testfall: PSO COMPUTE DIGITAL SIGNATURE (TC_PSO_COMPUTE_DIGITAL_SIGNATURE_FF_5)

2.392.1 Informationen

ID	TC_PSO_COMPUTE_DIGITAL_SIGNATURE_FF_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO COMPUTE DIGITAL SIGNATURE nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Dazu wird eine Kommandonachricht für PSO COMPUTE DIGITAL SIGNATURE zur Erzeugung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.392.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_02, VI_02_09

2.392.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- UNSUPPORTED_FU NCTION-1	Schlüssel unterstützt Algorithmus nicht
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

CN- NO_KEY_REFEREN CE-2	Key-Objekt ist ausgewählt
CN- KEY_NOT_FOUND- 2	KEY-Objekt kann gefunden werden
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN-KEY_INVALID- 2	Key-Daten sind vorhanden
CN- OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.392.4 APDU-Kommandos

ID: CM-PSO_COMPUTE_DIGITAL_SIGNATURE_FF_5						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.392.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.392.6 Verifikationen

ID	Beschreibung
VF- PSO_COMPUTE_DIGITAL_SIGNATURE-2	Es wird keine Signatur zurückgegeben.

2.393 Testfall: PSO COMPUTE DIGITAL SIGNATURE (TC_PSO_COMPUTE_DIGITAL_SIGNATURE_FF_6)

2.393.1 Informationen

ID	TC_PSO_COMPUTE_DIGITAL_SIGNATURE_FF_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO COMPUTE DIGITAL SIGNATURE nicht erfolgreich durchgeführt werden kann, wenn die Key-Daten nicht vorhanden sind. Dazu wird eine Kommandonachricht für PSO COMPUTE DIGITAL SIGNATURE zur Erzeugung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.393.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_02, VI_02_09

2.393.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_INVALID-1	Key-Daten sind nicht vorhanden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-	KEY-Objekt kann gefunden werden

KEY_NOT_FOUND-2	
CN-SECURITY_STATU S_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-UNSUPPORTED_FU NCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

2.393.4 APDU-Kommandos

ID: CM-PSO_COMPUTE_DIGITAL_SIGNATURE_FF_6						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.393.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6400	Das Testsystem antwortet mit '64 00'.

2.393.6 Verifikationen

ID	Beschreibung
VF-PSO_COMPUTE_DIGITAL_SIGNATURE-2	Es wird keine Signatur zurückgegeben.

2.394 Testfall: PSO COMPUTE DIGITAL SIGNATURE (TC_PSO_COMPUTE_DIGITAL_SIGNATURE_FF_7)

2.394.1 Informationen

ID	TC_PSO_COMPUTE_DIGITAL_SIGNATURE_FF_7
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO COMPUTE DIGITAL SIGNATURE nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Dazu wird eine Kommandonachricht für PSO COMPUTE DIGITAL SIGNATURE zur Erzeugung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.394.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_02, VI_02_09

2.394.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_DEACTIVATED-1	Key-Objekt befindet sich im Zustand "operational state - deactivated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt

CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-SECURITY_STATU S_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-UNSUPPORTED_FU NCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden

2.394.4 APDU-Kommandos

ID: CM-PSO_COMPUTE_DIGITAL_SIGNATURE_FF_7						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.394.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.394.6 Verifikationen

ID	Beschreibung
VF-PSO_COMPUTE_DIGITAL_SIGNATURE-2	Es wird keine Signatur zurückgegeben.

2.395 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_GF_1_1)

2.395.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_GF_1_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Die Durchführung erfolgt für die OID BrainpoolP256r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.395.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.395.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden

CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.395.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_GF_1_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.395.5 Erwartete Ergebnisse

ID	Beschreibung

RS-9000	Das Testsystem antwortet mit '90 00'.

2.395.6 Verifikationen

n/a

2.396 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_GF_1_2)

2.396.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_GF_1_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.396.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.396.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

CN- NO_KEY_REFEREN CE-2	Key-Objekt ist ausgewählt
CN- KEY_NOT_FOUND- 2	KEY-Objekt kann gefunden werden
CN- UNSUPPORTED_FU NCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID- 2	Key-Daten sind vorhanden
CN- OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN- OBJECT_ACTIVAT ED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.396.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_GF_1_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public

Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.396.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.396.6 Verifikationen

n/a

2.397 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_GF_1_3)

2.397.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_GF_1_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Die Durchführung erfolgt für die OID BrainpoolP512r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.397.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.397.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.397.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_GF_1_3						
CLA	INS	P1	P2	Lc	Data	Le

00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.397.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.397.6 Verifikationen

n/a

2.398 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_GF_1_4)

2.398.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_GF_1_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Die Durchführung erfolgt für die OID NIST P-256 (secp256r1). Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.398.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.398.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUS	Zugriffsregel ist erfüllt

S_NOT_SATISFIED-2	

2.398.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_GF_1_4						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.398.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.398.6 Verifikationen

n/a

2.399 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_GF_1_5)

2.399.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_GF_1_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE erfolgreich durchgeführt werden kann, sofern alle notwendigen

	Voraussetzungen erfüllt sind. Die Durchführung erfolgt für die OID NIST P-384 (secp384r1). Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.399.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.399.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.399.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_GF_1_5						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.399.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.399.6 Verifikationen

n/a

2.400 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_GF_2)

2.400.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_GF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE erfolgreich durchgeführt werden kann und die Signaturprüfung fehlschlägt. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.400.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.400.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden

CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.400.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_GF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.400.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6300	Das Testsystem antwortet mit '63 00'.

2.400.6 Verifikationen

n/a

2.401 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_1_1)

2.401.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_1_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Die Durchführung erfolgt für die OID BrainpoolP256r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.401.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.401.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"

CN- NO_KEY_REFEREN CE-2	Key-Objekt ist ausgewählt
CN- KEY_NOT_FOUND- 2	KEY-Objekt kann gefunden werden
CN- UNSUPPORTED_FU NCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID- 2	Key-Daten sind vorhanden
CN- OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN- OBJECT_ACTIVAT ED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.401.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_1_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public

Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.401.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.401.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.402 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_1_2)

2.402.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_1_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.402.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.402.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.402.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_1_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.402.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.402.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.403 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_1_3)

2.403.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_1_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn sich das

	Sicherheitsmodul im Zustand "terminiert" befindet. Die Durchführung erfolgt für die OID BrainpoolP512r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.403.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.403.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

CN- OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN- INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN- SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.403.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_1_3						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.403.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.403.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet

	werden.

2.404 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_1_4)

2.404.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_1_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Die Durchführung erfolgt für die OID NIST P-256 (secp256r1). Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.404.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.404.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt

CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.404.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_1_4						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.404.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.404.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.405 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_1_5)

2.405.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_1_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Die Durchführung erfolgt für die OID NIST P-384 (secp384r1). Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.405.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.405.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.405.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_1_5						
CLA	INS	P1	P2	Lc	Data	Le

00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.405.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.405.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.406 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_2_1)

2.406.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_2_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt nicht ausgewählt ist. Die Durchführung erfolgt für die OID BrainpoolP256r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.

Klassifizierung	Fehlerfall-Test

2.406.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.406.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-NO_KEY_REFERENCE-1	Key-Objekt ist nicht ausgewählt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.406.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_2_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.406.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6985	Das Testsystem antwortet mit '69 85'.

2.406.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.407 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_2_2)

2.407.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_2_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt nicht ausgewählt ist. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.407.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.407.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-NO_KEY_REFERENCE-1	Key-Objekt ist nicht ausgewählt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden

CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.407.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_2_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.407.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6985	Das Testsystem antwortet mit '69 85'.

2.407.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.408 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_2_3)

2.408.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_2_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt nicht ausgewählt ist. Die Durchführung erfolgt für die OID BrainpoolP512r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.408.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.408.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRE	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CTNESS	
CN- NO_KEY_REFEREN CE-1	Key-Objekt ist nicht ausgewählt
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- KEY_NOT_FOUND- 2	KEY-Objekt kann gefunden werden
CN- UNSUPPORTED_FU NCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID- 2	Key-Daten sind vorhanden
CN- OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN- OBJECT_ACTIVAT ED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.408.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_2_3						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.408.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6985	Das Testsystem antwortet mit '69 85'.

2.408.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.409 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_2_4)

2.409.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_2_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt nicht ausgewählt ist. Die Durchführung erfolgt für die OID NIST P-256 (secp256r1). Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.409.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.409.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-NO_KEY_REFERENCE-1	Key-Objekt ist nicht ausgewählt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUS	Zugriffsregel ist erfüllt

S_NOT_SATISFIED-2	

2.409.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_2_4						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.409.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6985	Das Testsystem antwortet mit '69 85'.

2.409.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.410 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_2_5)

2.410.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_2_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt nicht ausgewählt ist. Die Durchführung erfolgt für die OID NIST P-384 (secp384r1). Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.410.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.410.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-NO_KEY_REFERENCE-1	Key-Objekt ist nicht ausgewählt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden

CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.410.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_2_5						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.410.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6985	Das Testsystem antwortet mit '69 85'.

2.410.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.411 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_3_1)

2.411.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_3_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn das KEY-Objekt nicht gefunden wird. Die Durchführung erfolgt für die OID BrainpoolP256r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.411.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.411.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRE	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CTNESS	
CN-KEY_NOT_FOUND-1	KEY-Objekt kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.411.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_3_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.411.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.411.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.412 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_3_2)

2.412.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_3_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn das KEY-Objekt nicht gefunden wird. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.412.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.412.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	KEY-Objekt kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUS	Zugriffsregel ist erfüllt

S_NOT_SATISFIED-2	

2.412.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_3_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.412.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.412.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.413 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_3_3)

2.413.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_3_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn das KEY-Objekt nicht gefunden wird. Die Durchführung erfolgt für die OID BrainpoolP512r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.413.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.413.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	KEY-Objekt kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt

CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.413.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_3_3						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.413.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.413.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.414 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_3_4)

2.414.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_3_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn das KEY-Objekt nicht gefunden wird. Die Durchführung erfolgt für die OID NIST P-256 (secp256r1). Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.414.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.414.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRE	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CTNESS	
CN-KEY_NOT_FOUND-1	KEY-Objekt kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.414.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_3_4						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.414.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.414.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.415 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_3_5)

2.415.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_3_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn das KEY-Objekt nicht gefunden wird. Die Durchführung erfolgt für die OID NIST P-384 (secp384r1). Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.415.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.415.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	KEY-Objekt kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUS	Zugriffsregel ist erfüllt

S_NOT_SATISFIED-2	

2.415.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_3_5						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.415.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.415.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.416 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_4_1)

2.416.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_4_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für die OID BrainpoolP256r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.416.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.416.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt

CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.416.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_4_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.416.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.416.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.417 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_4_2)

2.417.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_4_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.417.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.417.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRE	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CTNESS	
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.417.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_4_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.417.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.417.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.418 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_4_3)

2.418.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_4_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für die OID BrainpoolP512r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.418.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.418.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUS	Zugriffsregel ist erfüllt

S_NOT_SATISFIED-2	

2.418.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_4_3						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.418.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.418.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.419 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_4_4)

2.419.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_4_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für die OID NIST P-256 (secp256r1). Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.419.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.419.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt

CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.419.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_4_4						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.419.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.419.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.420 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_4_5)

2.420.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_4_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für die OID NIST P-384 (secp384r1). Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.420.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.420.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRE	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CTNESS	
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.420.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_4_5						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.420.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.420.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.421 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_5_1)

2.421.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_5_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Key-Daten nicht vorhanden sind. Die Durchführung erfolgt für die OID BrainpoolP256r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.421.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.421.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_INVALID-1	Key-Daten sind nicht vorhanden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUS	Zugriffsregel ist erfüllt

S_NOT_SATISFIED-2	

2.421.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_5_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.421.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6400	Das Testsystem antwortet mit '64 00'.

2.421.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.422 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_5_2)

2.422.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_5_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Key-Daten nicht vorhanden sind. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.422.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.422.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_INVALID-1	Key-Daten sind nicht vorhanden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt

CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.422.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_5_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.422.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6400	Das Testsystem antwortet mit '64 00'.

2.422.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.423 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_5_3)

2.423.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_5_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Key-Daten nicht vorhanden sind. Die Durchführung erfolgt für die OID BrainpoolP512r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.423.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.423.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_INVALID-1	Key-Daten sind nicht vorhanden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.423.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_5_3						
CLA	INS	P1	P2	Lc	Data	Le

00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.423.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6400	Das Testsystem antwortet mit '64 00'.

2.423.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.424 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_5_4)

2.424.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_5_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Key-Daten nicht vorhanden sind. Die Durchführung erfolgt für die OID NIST P-256 (secp256r1). Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.

Klassifizierung	Fehlerfall-Test

2.424.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.424.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_INVALID-1	Key-Daten sind nicht vorhanden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.424.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_5_4						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.424.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6400	Das Testsystem antwortet mit '64 00'.

2.424.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.425 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_5_5)

2.425.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_5_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Key-Daten nicht vorhanden sind. Die Durchführung erfolgt für die OID NIST P-384 (secp384r1). Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.425.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.425.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_INVALID-1	Key-Daten sind nicht vorhanden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt

CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.425.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_5_5						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.425.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6400	Das Testsystem antwortet mit '64 00'.

2.425.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.426 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_6_1)

2.426.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_6_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Die Durchführung erfolgt für die OID BrainpoolP256r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.426.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.426.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_DEACTIVATED-1	Key-Objekt befindet sich im Zustand "operational state - deactivated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.426.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_6_1						
CLA	INS	P1	P2	Lc	Data	Le

00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.426.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.426.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.427 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_6_2)

2.427.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_6_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.

Klassifizierung	Fehlerfall-Test

2.427.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.427.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_DEACTIVATED-1	Key-Objekt befindet sich im Zustand "operational state - deactivated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.427.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_6_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.427.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.427.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.428 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_6_3)

2.428.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_6_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Die Durchführung erfolgt für die OID BrainpoolP512r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.428.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.428.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_DEACTIVATED-1	Key-Objekt befindet sich im Zustand "operational state - deactivated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt

CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.428.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_6_3						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.428.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

2.428.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.429 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_6_4)

2.429.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_6_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Die Durchführung erfolgt für die OID NIST P-256 (secp256r1). Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.429.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.429.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRE	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CTNESS	
CN- OBJECT_DEACTIVATED-1	Key-Objekt befindet sich im Zustand "operational state - deactivated"
CN- INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN- KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN- UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN- OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN- INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN- SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.429.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_6_4						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.429.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.429.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.430 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_6_5)

2.430.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_6_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Die Durchführung erfolgt für die OID NIST P-384 (secp384r1). Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.430.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.430.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_DEACTIVATED-1	Key-Objekt befindet sich im Zustand "operational state - deactivated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUS	Zugriffsregel ist erfüllt

S_NOT_SATISFIED-2	

2.430.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_6_5						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.430.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.430.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.431 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_7_1)

2.431.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_7_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn sich das PIN-Objekt im Zustand "operational state - activated" befindet. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.431.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.431.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_ACTIVATED-1	PIN-Objekt befindet sich im Zustand "operational state - activated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt

CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.431.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_7_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.431.5 Erwartete Ergebnisse

ID	Beschreibung

RS-9000	Das Testsystem antwortet mit '90 00'.

2.431.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.432 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_7_2)

2.432.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_7_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn sich das PIN-Objekt im Zustand "operational state - activated" befindet. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.432.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.432.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRE	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CTNESS	
CN-OBJECT_ACTIVATED-1	PIN-Objekt befindet sich im Zustand "operational state - activated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.432.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_7_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.432.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.432.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.433 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_7_3)

2.433.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_7_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn sich das PIN-Objekt im Zustand "operational state - activated" befindet. Die Durchführung erfolgt für die OID BrainpoolP512r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.433.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.433.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_ACTIVATED-1	PIN-Objekt befindet sich im Zustand "operational state - activated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUS	Zugriffsregel ist erfüllt

S_NOT_SATISFIED-2	

2.433.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_7_3						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.433.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.433.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.434 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_7_4)

2.434.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_7_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn sich das PIN-Objekt im Zustand "operational state - activated" befindet. Die Durchführung erfolgt für die OID NIST P-256 (secp256r1). Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.434.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.434.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_ACTIVATED-1	PIN-Objekt befindet sich im Zustand "operational state - activated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt

CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.434.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_7_4						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.434.5 Erwartete Ergebnisse

ID	Beschreibung

RS-9000	Das Testsystem antwortet mit '90 00'.

2.434.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.435 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_7_5)

2.435.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_7_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn sich das PIN-Objekt im Zustand "operational state - activated" befindet. Die Durchführung erfolgt für die OID NIST P-384 (secp384r1). Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.435.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.435.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRE	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CTNESS	
CN-OBJECT_ACTIVATED-1	PIN-Objekt befindet sich im Zustand "operational state - activated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.435.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_7_5						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.435.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.435.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.436 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_1)

2.436.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_8_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 5f 29. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.436.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.436.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 5f 29)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-SECURITY_STATUS	Zugriffsregel ist erfüllt

S_NOT_SATISFIED-2	

2.436.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_8_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.436.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.436.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.437 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_2)

2.437.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_8_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 5f 29 leer ist. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.437.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.437.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (5f 29-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt

CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.437.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_8_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.437.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.437.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.438 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_3)

2.438.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_8_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 5f 29 fehlt. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.438.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.438.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRE	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CTNESS	
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (5f 29-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.438.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_8_3						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.438.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.438.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.439 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_4)

2.439.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_8_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschen Längenangaben im Tag 5f 29. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.439.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.439.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falscher Längenangabe im Tag 5f 29)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-SECURITY_STATUS	Zugriffsregel ist erfüllt

S_NOT_SATISFIED-2	

2.439.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_8_4						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.439.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.439.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.440 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_5)

2.440.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_8_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 06. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.440.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.440.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 06)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt

CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.440.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_8_5						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.440.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.440.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.441 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_6)

2.441.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_8_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 06 leer ist. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.441.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.441.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRE	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CTNESS	
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (06-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.441.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_8_6						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.441.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.441.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.442 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_7)

2.442.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_8_7
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 06 fehlt. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.442.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.442.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (06-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-SECURITY_STATUS	Zugriffsregel ist erfüllt

S_NOT_SATISFIED-2	

2.442.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_8_7						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.442.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.442.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.443 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_8)

2.443.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_8_8
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschen Längenangaben im Tag 06. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.443.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.443.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falscher Längenangabe im Tag 06)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt

CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.443.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_8_8						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.443.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.443.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.444 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_9)

2.444.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_8_9
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 86. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.444.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.444.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRE	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CTNESS	
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 86)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.444.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_8_9						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.444.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.444.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.445 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_10)

2.445.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_8_10
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 86 leer ist. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.445.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.445.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (86-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-SECURITY_STATUS	Zugriffsregel ist erfüllt

S_NOT_SATISFIED-2	

2.445.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_8_10						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.445.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.445.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.446 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_11)

2.446.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_8_11
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 86 fehlt. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.446.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.446.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (86-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt

CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.446.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_8_11						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.446.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.446.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.447 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_12)

2.447.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_8_12
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschen Längenangaben im Tag 86. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.447.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.447.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRE	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CTNESS	
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falscher Längenangabe im Tag 86)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.447.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_8_12						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.447.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.447.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.448 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_13)

2.448.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_8_13
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 5f 20. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.448.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.448.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 5f 20)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-SECURITY_STATUS	Zugriffsregel ist erfüllt

S_NOT_SATISFIED-2	

2.448.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_8_13						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.448.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.448.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.449 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_14)

2.449.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_8_14
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 5f 20 leer ist. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.449.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.449.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (5f 20-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt

CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.449.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_8_14						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.449.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.449.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.450 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_15)

2.450.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_8_15
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 5f 20 fehlt. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.450.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.450.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRE	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CTNESS	
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (5f 20-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.450.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_8_15						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.450.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.450.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.451 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_16)

2.451.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_8_16
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschen Längenangaben im Tag 5f 20. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.451.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.451.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falscher Längenangabe im Tag 5f 20)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-SECURITY_STATUS	Zugriffsregel ist erfüllt

S_NOT_SATISFIED-2	

2.451.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_8_16						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.451.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.451.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.452 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_17)

2.452.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_8_17
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 5f 37. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.452.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.452.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 5f 37)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt

CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.452.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_8_17						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.452.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.452.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.453 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_18)

2.453.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_8_18
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 5f 37 leer ist. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.453.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.453.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRE	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CTNESS	
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (5f 37-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.453.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_8_18						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.453.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.453.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.454 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_19)

2.454.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_8_19
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 5f 37 fehlt. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.454.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.454.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (5f 37-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-SECURITY_STATUS	Zugriffsregel ist erfüllt

S_NOT_SATISFIED-2	

2.454.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_8_19						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.454.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.454.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.455 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_20)

2.455.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_8_20
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschen Längenangaben im Tag 5f 37. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.455.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.455.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falscher Längenangabe im Tag 5f 37)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt

CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.455.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_8_20						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.455.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.455.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.456 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_21)

2.456.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_8_21
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 7f 4e. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.456.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.456.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRE	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CTNESS	
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 7f 4e)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.456.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_8_21						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.456.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.456.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.457 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_22)

2.457.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_8_22
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 7f 4e leer ist. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.457.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.457.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (7f 4e-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-SECURITY_STATUS	Zugriffsregel ist erfüllt

S_NOT_SATISFIED-2	

2.457.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_8_22						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.457.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.457.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.458 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_23)

2.458.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_8_23
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 7f 4e fehlt. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.458.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.458.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (7f 4e-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt

CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.458.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_8_23						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.458.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.458.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.459 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_8_24)

2.459.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_8_24
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschen Längenangaben im Tag 7f 4e. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.459.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.459.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRE	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CTNESS	
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falscher Längenangabe im Tag 7f 4e)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.459.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_8_24						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.459.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.459.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.460 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_9_1)

2.460.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_9_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.460.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.460.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit

INCORRECT_PARA METERS-2	richtigem Tag für 5f 29)

2.460.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_9_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.460.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.460.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.461 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_9_2)

2.461.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_9_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.461.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.461.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFEREN	Key-Objekt ist ausgewählt

CE-2	
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)

2.461.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_9_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.461.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.461.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.462 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_9_3)

2.462.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_9_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Die Durchführung erfolgt für die OID BrainpoolP512r1. Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.462.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.462.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)

2.462.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_9_3						
CLA	INS	P1	P2	Lc	Data	Le

00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.462.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.462.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.463 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_9_4)

2.463.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_9_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Die Durchführung erfolgt für die OID NIST P-256 (secp256r1). Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.

Klassifizierung	Fehlerfall-Test

2.463.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.463.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"

ED-2	
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)

2.463.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_9_4						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.463.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.463.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.464 Testfall: PSO VERIFY CERTIFICATE (TC_PSO_VERIFY_CERTIFICATE_FF_9_5)

2.464.1 Informationen

ID	TC_PSO_VERIFY_CERTIFICATE_FF_9_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY CERTIFICATE nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Die Durchführung erfolgt für die OID NIST P-384 (secp384r1). Dazu wird eine Kommandonachricht für PSO VERIFY CERTIFICATE zum Importieren von öffentlichen Schlüsseln an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.464.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.4

Der Testfall wird in folgenden Use-Cases referenziert: VI_02_07, VI_02_08

2.464.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCED	Key-Objekt ist ausgewählt

CE-2	
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-OBJECT_ACTIVATED-2	PIN-Objekt befindet sich nicht im Zustand "operational state - activated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (Datenobjekt mit richtigem Tag für 5f 29)

2.464.4 APDU-Kommandos

ID: CM-PSO_VERIFY_CERTIFICATE_FF_9_5						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	7f 4e LL [5f 29 LL [XX...XX] 7f 49 LL [06 LL [XX...XX] 86 LL [XX...XX]] 5f 20 LL [XX...XX]] 5f 37 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

2.464.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.464.6 Verifikationen

ID	Beschreibung
VF-PSO_VERIFY_CERTIFICATE-1	Der Public-Key kann in nachfolgenden Operationen nicht erfolgreich verwendet werden.

2.465 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_GF_1)

2.465.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.465.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.465.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.465.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_GF_1

CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.465.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.465.6 Verifikationen

n/a

2.466 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_GF_2_1)

2.466.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_GF_2_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key erfolgreich durchgeführt werden kann und die Signaturprüfung fehlschlägt. Die Durchführung erfolgt für die OID BrainpoolP256r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.466.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.466.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.466.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_GF_2_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.466.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6300	Das Testsystem antwortet mit '63 00'.

2.466.6 Verifikationen

n/a

2.467 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_GF_2_2)

2.467.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_GF_2_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key erfolgreich durchgeführt werden kann und die Signaturprüfung fehlschlägt. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche

	Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.467.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.467.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-	Zugriffsregel ist erfüllt

SECURITY_STATUS_NOT_SATISFIED-2	

2.467.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_GF_2_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.467.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6300	Das Testsystem antwortet mit '63 00'.

2.467.6 Verifikationen

n/a

2.468 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_GF_2_3)

2.468.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_GF_2_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key erfolgreich durchgeführt

	werden kann und die Signaturprüfung fehlschlägt. Die Durchführung erfolgt für die OID BrainpoolP512r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.468.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.468.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

CN- INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.468.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_GF _2_3						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.468.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6300	Das Testsystem antwortet mit '63 00'.

2.468.6 Verifikationen

n/a

2.469 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_GF_2_4)

2.469.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_GF_2_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key erfolgreich durchgeführt werden kann und die Signaturprüfung fehlschlägt. Die Durchführung erfolgt für die OID NIST P-256 (secp256r1). Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.469.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.469.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFEREN	Key-Objekt ist ausgewählt

CE-2	
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.469.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_GF_2_4						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.469.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6300	Das Testsystem antwortet mit '63 00'.

2.469.6 Verifikationen

n/a

2.470 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_GF_2_5)

2.470.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_GF_2_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key erfolgreich durchgeführt werden kann und die Signaturprüfung fehlschlägt. Die Durchführung erfolgt für die OID NIST P-384 (secp384r1). Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.470.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.470.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

INSTRUCTION_NO T_SUPPORTED-2	
CN- NO_KEY_REFEREN CE-2	Key-Objekt ist ausgewählt
CN- KEY_NOT_FOUND- 2	KEY-Objekt kann gefunden werden
CN- UNSUPPORTED_FU NCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID- 2	Key-Daten sind vorhanden
CN- OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.470.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_GF _2_5						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.470.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6300	Das Testsystem antwortet mit '63 00'.

2.470.6 Verifikationen

n/a

2.471 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_1_1)

2.471.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_1_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Die Durchführung erfolgt für die OID BrainpoolP256r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.471.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.471.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.471.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_1_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.471.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.471.6 Verifikationen

n/a

2.472 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_1_2)

2.472.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_1_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.472.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.472.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.472.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_1_2

CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.472.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.472.6 Verifikationen

n/a

2.473 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_1_3)

2.473.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_1_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Die Durchführung erfolgt für die OID BrainpoolP512r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.473.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.473.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.473.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_1_3						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.473.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.473.6 Verifikationen

n/a

2.474 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_1_4)

2.474.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_1_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Die Durchführung erfolgt für die OID NIST P-256 (secp256r1). Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die

	erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.474.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.474.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.474.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_1_4						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.474.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.474.6 Verifikationen

n/a

2.475 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_1_5)

2.475.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_1_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL

	SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Die Durchführung erfolgt für die OID NIST P-384 (secp384r1). Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.475.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.475.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

OBJECT_DEACTIVATED-2	
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.475.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_1_5						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.475.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.475.6 Verifikationen

n/a

2.476 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_2_1)

2.476.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_2_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt nicht ausgewählt ist. Die Durchführung erfolgt für die OID BrainpoolP256r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.476.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.476.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-NO_KEY_REFERENCE-1	Key-Objekt ist nicht ausgewählt
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.476.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_2_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.476.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6985	Das Testsystem antwortet mit '69 85'.

2.476.6 Verifikationen

n/a

2.477 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_2_2)

2.477.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_2_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt nicht ausgewählt ist. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.477.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.477.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-	Key-Objekt ist nicht ausgewählt

NO_KEY_REFEREN CE-1	
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- KEY_NOT_FOUND- 2	KEY-Objekt kann gefunden werden
CN- UNSUPPORTED_FU NCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID- 2	Key-Daten sind vorhanden
CN- OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.477.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF _2_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.477.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6985	Das Testsystem antwortet mit '69 85'.

2.477.6 Verifikationen

n/a

2.478 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_2_3)

2.478.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_2_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt nicht ausgewählt ist. Die Durchführung erfolgt für die OID BrainpoolP512r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.478.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.478.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-NO_KEY_REFERENCE-1	Key-Objekt ist nicht ausgewählt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.478.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_2_3						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.478.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6985	Das Testsystem antwortet mit '69 85'.

2.478.6 Verifikationen

n/a

2.479 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_2_4)

2.479.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_2_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt nicht ausgewählt ist. Die Durchführung erfolgt für die OID NIST P-256 (secp256r1). Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.479.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.479.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-NO_KEY_REFERENCE-1	Key-Objekt ist nicht ausgewählt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.479.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_2_4

CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.479.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6985	Das Testsystem antwortet mit '69 85'.

2.479.6 Verifikationen

n/a

2.480 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_2_5)

2.480.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_2_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt nicht ausgewählt ist. Die Durchführung erfolgt für die OID NIST P-384 (secp384r1). Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.480.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.480.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-NO_KEY_REFERENCE-1	Key-Objekt ist nicht ausgewählt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.480.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_2_5						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.480.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6985	Das Testsystem antwortet mit '69 85'.

2.480.6 Verifikationen

n/a

2.481 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_3_1)

2.481.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_3_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn das KEY-Objekt nicht gefunden wird. Die Durchführung erfolgt für die OID BrainpoolP256r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche

	Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.481.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.481.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	KEY-Objekt kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.481.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_3_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.481.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.481.6 Verifikationen

n/a

2.482 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_3_2)

2.482.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_3_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL

	SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn das KEY-Objekt nicht gefunden wird. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.482.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.482.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	KEY-Objekt kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

OBJECT_DEACTIVATED-2	
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.482.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_3_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.482.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.482.6 Verifikationen

n/a

2.483 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_3_3)

2.483.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_3_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn das KEY-Objekt nicht gefunden wird. Die Durchführung erfolgt für die OID BrainpoolP512r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.483.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.483.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	KEY-Objekt kann nicht gefunden werden
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN- NO_KEY_REFEREN CE-2	Key-Objekt ist ausgewählt
CN- UNSUPPORTED_FU NCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID- 2	Key-Daten sind vorhanden
CN- OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.483.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF _3_3						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.483.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.483.6 Verifikationen

n/a

2.484 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_3_4)

2.484.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_3_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn das KEY-Objekt nicht gefunden wird. Die Durchführung erfolgt für die OID NIST P-256 (secp256r1). Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.484.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.484.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-	KEY-Objekt kann nicht gefunden werden

KEY_NOT_FOUND-1	
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.484.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_3_4						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.484.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.484.6 Verifikationen

n/a

2.485 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_3_5)

2.485.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_3_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn das KEY-Objekt nicht gefunden wird. Die Durchführung erfolgt für die OID NIST P-384 (secp384r1). Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.485.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.485.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_NOT_FOUND-1	KEY-Objekt kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.485.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_3_5						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.485.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A88	Das Testsystem antwortet mit '6a 88'.

2.485.6 Verifikationen

n/a

2.486 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_4_1)

2.486.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_4_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für die OID BrainpoolP256r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.486.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.486.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.486.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_4_1

CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.486.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.486.6 Verifikationen

n/a

2.487 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_4_2)

2.487.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_4_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.487.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.487.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.487.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_4_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.487.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.487.6 Verifikationen

n/a

2.488 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_4_3)

2.488.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_4_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für die OID BrainpoolP512r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche

	Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.488.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.488.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.488.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_4_3						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.488.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.488.6 Verifikationen

n/a

2.489 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_4_4)

2.489.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_4_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL

	SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für die OID NIST P-256 (secp256r1). Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.489.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.489.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

OBJECT_DEACTIVATED-2	
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.489.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_4_4						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.489.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.489.6 Verifikationen

n/a

2.490 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_4_5)

2.490.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_4_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für die OID NIST P-384 (secp384r1). Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.490.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.490.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN- NO_KEY_REFEREN CE-2	Key-Objekt ist ausgewählt
CN- KEY_NOT_FOUND- 2	KEY-Objekt kann gefunden werden
CN-KEY_INVALID- 2	Key-Daten sind vorhanden
CN- OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.490.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF _4_5						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.490.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.490.6 Verifikationen

n/a

2.491 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_5_1)

2.491.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_5_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Key-Daten nicht vorhanden sind. Die Durchführung erfolgt für die OID BrainpoolP256r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.491.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.491.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_INVALID-	Key-Daten sind nicht vorhanden

1	
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.491.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_5_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.491.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6400	Das Testsystem antwortet mit '64 00'.

2.491.6 Verifikationen

n/a

2.492 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_5_2)

2.492.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_5_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Key-Daten nicht vorhanden sind. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.492.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.492.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_INVALID-1	Key-Daten sind nicht vorhanden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.492.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_5_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.492.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6400	Das Testsystem antwortet mit '64 00'.

2.492.6 Verifikationen

n/a

2.493 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_5_3)

2.493.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_5_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Key-Daten nicht vorhanden sind. Die Durchführung erfolgt für die OID BrainpoolP512r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.493.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.493.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_INVALID-1	Key-Daten sind nicht vorhanden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.493.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_5_3

CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.493.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6400	Das Testsystem antwortet mit '64 00'.

2.493.6 Verifikationen

n/a

2.494 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_5_4)

2.494.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_5_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Key-Daten nicht vorhanden sind. Die Durchführung erfolgt für die OID NIST P-256 (secp256r1). Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.494.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.494.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_INVALID-1	Key-Daten sind nicht vorhanden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.494.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_5_4						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.494.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6400	Das Testsystem antwortet mit '64 00'.

2.494.6 Verifikationen

n/a

2.495 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_5_5)

2.495.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_5_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Key-Daten nicht vorhanden sind. Die Durchführung erfolgt für die OID NIST P-384 (secp384r1). Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche

	Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.495.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.495.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-KEY_INVALID-1	Key-Daten sind nicht vorhanden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.495.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_5_5						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.495.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6400	Das Testsystem antwortet mit '64 00'.

2.495.6 Verifikationen

n/a

2.496 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_6_1)

2.496.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_6_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL

	SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Die Durchführung erfolgt für die OID BrainpoolP256r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.496.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.496.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_DEACTIVATED-1	Key-Objekt befindet sich im Zustand "operational state - deactivated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus

CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATU S_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.496.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_6_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.496.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.496.6 Verifikationen

n/a

2.497 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_6_2)

2.497.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_6_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.497.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.497.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_DEACTIVATED-1	Key-Objekt befindet sich im Zustand "operational state - deactivated"
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN- NO_KEY_REFEREN CE-2	Key-Objekt ist ausgewählt
CN- KEY_NOT_FOUND- 2	KEY-Objekt kann gefunden werden
CN- UNSUPPORTED_FU NCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID- 2	Key-Daten sind vorhanden
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.497.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF _6_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.497.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.497.6 Verifikationen

n/a

2.498 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_6_3)

2.498.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_6_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Die Durchführung erfolgt für die OID BrainpoolP512r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.498.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.498.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-	Key-Objekt befindet sich im Zustand "operational state - deactivated"

OBJECT_DEACTIVATED-1	
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.498.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_6_3						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.498.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.498.6 Verifikationen

n/a

2.499 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_6_4)

2.499.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_6_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Die Durchführung erfolgt für die OID NIST P-256 (secp256r1). Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.499.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.499.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_DEACTIVATED-1	Key-Objekt befindet sich im Zustand "operational state - deactivated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.499.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_6_4						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.499.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.499.6 Verifikationen

n/a

2.500 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_6_5)

2.500.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_6_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn das Key-Objekt sich im Zustand "operational state - deactivated" befindet. Die Durchführung erfolgt für die OID NIST P-384 (secp384r1). Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.500.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.500.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OBJECT_DEACTIVATED-1	Key-Objekt befindet sich im Zustand "operational state - deactivated"
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.500.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_6_5

CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.500.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.500.6 Verifikationen

n/a

2.501 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_1)

2.501.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 90 fehlt. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.501.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.501.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (90-Objekt fehlt)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.501.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.501.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.501.6 Verifikationen

n/a

2.502 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_2)

2.502.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 90 leer ist. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche

	Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.502.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.502.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (90-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.502.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 00 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.502.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.502.6 Verifikationen

n/a

2.503 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_3)

2.503.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL

	SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschen Längenangaben im Tag 90. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.503.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.503.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falscher Längenangabe im Tag 90)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus

CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.503.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_3						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.503.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.503.6 Verifikationen

n/a

2.504 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_4)

2.504.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 90. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.504.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.504.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 90)
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN- NO_KEY_REFEREN CE-2	Key-Objekt ist ausgewählt
CN- KEY_NOT_FOUND- 2	KEY-Objekt kann gefunden werden
CN- UNSUPPORTED_FU NCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID- 2	Key-Daten sind vorhanden
CN- OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.504.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF _7_4						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.504.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.504.6 Verifikationen

n/a

2.505 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_5)

2.505.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 9e fehlt. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.505.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.505.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-	Parameter im Kommando-Datenfeld sind nicht korrekt (9e-Objekt fehlt)

INCORRECT_PARAMETERS-1	
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.505.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_5						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.505.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.505.6 Verifikationen

n/a

2.506 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_6)

2.506.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 9e leer ist. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.506.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.506.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (9e-Objekt ist leer)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.506.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_6						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e 00	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.506.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.506.6 Verifikationen

n/a

2.507 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_7)

2.507.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_7
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschen Längenangaben im Tag 9e. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.507.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.507.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falscher Längenangabe im Tag 9e)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.507.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_7

CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.507.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.507.6 Verifikationen

n/a

2.508 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_8)

2.508.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_8
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 9e. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.508.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.508.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 9e)
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.508.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_7_8						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.508.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.508.6 Verifikationen

n/a

2.509 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_8_1)

2.509.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_8_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die

	erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.509.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.509.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"

CN- INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)

2.509.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_8_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.509.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.509.6 Verifikationen

n/a

2.510 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_8_2)

2.510.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_8_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich

	durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.510.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.510.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus

CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)

2.510.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_8_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.510.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.510.6 Verifikationen

n/a

2.511 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_8_3)

2.511.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_8_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Die Durchführung erfolgt für die OID BrainpoolP512r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.511.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.511.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

INSTRUCTION_NO T_SUPPORTED-2	
CN- NO_KEY_REFEREN CE-2	Key-Objekt ist ausgewählt
CN- KEY_NOT_FOUND- 2	KEY-Objekt kann gefunden werden
CN- UNSUPPORTED_FU NCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID- 2	Key-Daten sind vorhanden
CN- OBJECT_DEACTIV ATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)

2.511.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF _8_3						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.511.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.511.6 Verifikationen

n/a

2.512 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_8_4)

2.512.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_8_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Die Durchführung erfolgt für die OID NIST P-256 (secp256r1). Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.512.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.512.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-	Zugriffsregel ist nicht erfüllt

SECURITY_STATUS_NOT_SATISFIED-1	
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)

2.512.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_8_4						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.512.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.512.6 Verifikationen

n/a

2.513 Testfall: PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_8_5)

2.513.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_8_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Die Durchführung erfolgt für die OID NIST P-384 (secp384r1). Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE ohne Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.513.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11b

2.513.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_KEY_REFERENCE-2	Key-Objekt ist ausgewählt
CN-KEY_NOT_FOUND-2	KEY-Objekt kann gefunden werden
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-KEY_INVALID-2	Key-Daten sind vorhanden
CN-OBJECT_DEACTIVATED-2	Key-Objekt befindet sich nicht im Zustand "operational state - deactivated"
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)

2.513.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITHOUT_TRANSFER_OF_PUBLIC_KEY_FF_8_5						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	90 LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

2.513.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.513.6 Verifikationen

n/a

2.514 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_GF_1)

2.514.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.514.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.514.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.514.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.514.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.514.6 Verifikationen

n/a

2.515 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_GF_2_1)

2.515.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_GF_2_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key erfolgreich durchgeführt werden kann und die Signaturprüfung fehlschlägt. Die Durchführung erfolgt für die OID BrainpoolP256r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.515.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.515.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- UNSUPPORTED_FU NCTION-2	Schlüssel unterstützt Algorithmus
CN- INCORRECT_PARA METERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.515.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_GF_2_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.515.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6300	Das Testsystem antwortet mit '63 00'.

2.515.6 Verifikationen

n/a

2.516 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_GF_2_2)

2.516.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_GF_2_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key erfolgreich durchgeführt werden kann und die Signaturprüfung fehlschlägt. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.516.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.516.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.516.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_GF_2_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.516.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6300	Das Testsystem antwortet mit '63 00'.

2.516.6 Verifikationen

n/a

2.517 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_GF_2_3)

2.517.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_GF_2_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key erfolgreich durchgeführt werden kann und die Signaturprüfung fehlschlägt. Die Durchführung erfolgt für die OID BrainpoolP512r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.517.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.517.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus

CN- INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.517.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_GF_2_3						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.517.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6300	Das Testsystem antwortet mit '63 00'.

2.517.6 Verifikationen

n/a

2.518 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_GF_2_4)

2.518.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_GF_2_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key erfolgreich durchgeführt werden kann und die Signaturprüfung fehlschlägt. Die Durchführung erfolgt für die OID NIST P-256 (secp256r1). Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.518.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.518.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-UNSUPPORTED_FUNCTION	Schlüssel unterstützt Algorithmus

NCTION-2	
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.518.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_GF_2_4						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.518.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6300	Das Testsystem antwortet mit '63 00'.

2.518.6 Verifikationen

n/a

2.519 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_GF_2_5)

2.519.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_GF_2_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key erfolgreich durchgeführt werden kann und die Signaturprüfung fehlschlägt. Die Durchführung erfolgt für die OID NIST P-384 (secp384r1). Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.519.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.519.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-UNSUPPORTED_FUNCTION	Schlüssel unterstützt Algorithmus

NCTION-2	
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.519.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_GF_2_5						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.519.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6300	Das Testsystem antwortet mit '63 00'.

2.519.6 Verifikationen

n/a

2.520 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_1_1)

2.520.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_1_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Die Durchführung erfolgt für die OID BrainpoolP256r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.520.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.520.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-UNSUPPORTED_FUNCTION	Schlüssel unterstützt Algorithmus

NCTION-2	
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.520.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_1_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.520.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.520.6 Verifikationen

n/a

2.521 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_1_2)

2.521.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_1_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.521.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.521.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-UNSUPPORTED_FUNCTION	Schlüssel unterstützt Algorithmus

NCTION-2	
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.521.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_1_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.521.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.521.6 Verifikationen

n/a

2.522 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_1_3)

2.522.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_1_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Die Durchführung erfolgt für die OID BrainpoolP512r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.522.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.522.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-UNSUPPORTED_FUNCTION	Schlüssel unterstützt Algorithmus

NCTION-2	
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.522.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_1_3						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.522.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.522.6 Verifikationen

n/a

2.523 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_1_4)

2.523.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_1_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Die Durchführung erfolgt für die OID NIST P-256 (secp256r1). Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.523.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.523.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-UNSUPPORTED_FUNCTION	Schlüssel unterstützt Algorithmus

NCTION-2	
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.523.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_1_4						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.523.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.523.6 Verifikationen

n/a

2.524 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_1_5)

2.524.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_1_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Die Durchführung erfolgt für die OID NIST P-384 (secp384r1). Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.524.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.524.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-UNSUPPORTED_FUNCTION	Schlüssel unterstützt Algorithmus

NCTION-2	
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

2.524.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_1_5						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.524.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.524.6 Verifikationen

n/a

2.525 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_2_1)

2.525.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_2_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für die OID BrainpoolP256r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.525.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.525.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATU S_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.525.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_2_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.525.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.525.6 Verifikationen

n/a

2.526 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_2_2)

2.526.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_2_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.526.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.526.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATU S_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.526.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_2_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.526.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.526.6 Verifikationen

n/a

2.527 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_2_3)

2.527.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_2_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für die OID BrainpoolP512r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.527.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.527.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATU S_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.527.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_2_3						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.527.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.527.6 Verifikationen

n/a

2.528 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_2_4)

2.528.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_2_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für die OID NIST P-256 (secp256r1). Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.528.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.528.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATU S_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.528.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_2_4						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.528.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.528.6 Verifikationen

n/a

2.529 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_2_5)

2.529.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_2_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn der Schlüssel den Algorithmus nicht unterstützt. Die Durchführung erfolgt für die OID NIST P-384 (secp384r1). Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.529.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.529.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-UNSUPPORTED_FUNCTION-1	Schlüssel unterstützt Algorithmus nicht
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)
CN-SECURITY_STATU S_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.529.4 APDU-Kommandos

ID: CM- PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_2_5						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.529.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A81	Das Testsystem antwortet mit '6a 81'.

2.529.6 Verifikationen

n/a

2.530 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_1)

2.530.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 90 fehlt. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.530.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.530.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (90-Objekt fehlt)
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.530.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.530.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.530.6 Verifikationen

n/a

2.531 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_2)

2.531.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 90 leer ist. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.531.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.531.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (90-Objekt ist leer)
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.531.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 00 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.531.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.531.6 Verifikationen

n/a

2.532 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_3)

2.532.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschen Längenangaben im Tag 90. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.532.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.532.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falscher Längenangabe im Tag 90)
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.532.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_3						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.532.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.532.6 Verifikationen

n/a

2.533 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_4)

2.533.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 90. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.533.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.533.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 90)
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.533.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_4						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.533.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.533.6 Verifikationen

n/a

2.534 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_5)

2.534.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 9e fehlt. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.534.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.534.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (9e-Objekt fehlt)
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.534.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_5						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.534.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.534.6 Verifikationen

n/a

2.535 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_6)

2.535.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. In diesem Testfall bedeutet inkorrekt, dass das Objekt 9e leer ist. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.535.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.535.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (9e-Objekt ist leer)
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.535.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_6						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e 00	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.535.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.535.6 Verifikationen

n/a

2.536 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_7)

2.536.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_7
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschen Längenangaben im Tag 9e. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.536.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.536.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falscher Längenangabe im Tag 9e)
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.536.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_7						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.536.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.536.6 Verifikationen

n/a

2.537 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_8)

2.537.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_8
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Parameter im Kommando-Datenfeld inkorrekt sind. Die Durchführung erfolgt mit falschem Tag 9e. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.537.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.537.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INCORRECT_PARAMETERS-1	Parameter im Kommando-Datenfeld sind nicht korrekt (Datenobjekt mit falschem Tag für 9e)
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

T_SUPPORTED-2	
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-SECURITY_STATUSS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.537.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_3_8						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.537.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A80	Das Testsystem antwortet mit '6a 80'.

2.537.6 Verifikationen

n/a

2.538 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_4_1)

2.538.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_4_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.538.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.538.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

INSTRUCTION_NOT_SUPPORTED-2	
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)

2.538.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_4_1						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.538.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.538.6 Verifikationen

n/a

2.539 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_4_2)

2.539.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_4_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Die Durchführung erfolgt für die OID BrainpoolP384r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.539.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.539.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

INSTRUCTION_NOT_SUPPORTED-2	
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)

2.539.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_4_2						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.539.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.539.6 Verifikationen

n/a

2.540 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_4_3)

2.540.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_4_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Die Durchführung erfolgt für die OID BrainpoolP512r1. Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.540.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.540.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

INSTRUCTION_NOT_SUPPORTED-2	
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)

2.540.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_4_3						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.540.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.540.6 Verifikationen

n/a

2.541 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_4_4)

2.541.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_4_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Die Durchführung erfolgt für die OID NIST P-256 (secp256r1). Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.541.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.541.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

INSTRUCTION_NOT_SUPPORTED-2	
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)

2.541.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_4_4						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.541.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.541.6 Verifikationen

n/a

2.542 Testfall: PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key (TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_4_5)

2.542.1 Informationen

ID	TC_PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_4_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Die Durchführung erfolgt für die OID NIST P-384 (secp384r1). Dazu wird eine Kommandonachricht für PSO VERIFY DIGITAL SIGNATURE mit Übergabe des Public-Key zur Prüfung von Signaturen an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.542.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.5.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_05_04b, VI_02_11a

2.542.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

INSTRUCTION_NOT_SUPPORTED-2	
CN-UNSUPPORTED_FUNCTION-2	Schlüssel unterstützt Algorithmus
CN-INCORRECT_PARAMETERS-2	Parameter im Kommando-Datenfeld sind korrekt (90-Objekt fehlt nicht)

2.542.4 APDU-Kommandos

ID: CM-PSO_VERIFY_DIGITAL_SIGNATURE_WITH_TRANSFER_OF_PUBLIC_KEY_FF_4_5						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	06 LL [XX...XX] 90 LL [XX...XX] 9c LL [XX...XX] 9e LL [XX...XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

2.542.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.542.6 Verifikationen

n/a

2.543 Testfall: READ BINARY ohne SFI (TC_READ_BINARY_WITHOUT_SFI_GF_1_1)

2.543.1 Informationen

ID	TC_READ_BINARY_WITHOUT_SFI_GF_1_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ BINARY ohne SFI erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für READ BINARY ohne SFI zum Auslesen eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.543.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_01a, VI_02_12a

2.543.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- NO_CURRENT_EF- 2	Das EF ist ausgewählt
CN- WRONG_FILE_TYP E-2	Ausgewähltes EF ist transparent

CN-OFFSET_TOO_BIG-2	Parameter "Offset" in Kommando-APDU ist nicht zu groß

2.543.4 APDU-Kommandos

ID: CM-READ_BINARY_WITHOUT_SFI_GF_1_1						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.543.5 Erwartete Ergebnisse

ID	Beschreibung
RS-31EA	XX...XX 90 00

2.543.6 Verifikationen

ID	Beschreibung
VF-READ_BINARY_WITHOUT_SFI-1	Die ausgelesenen Daten stimmen mit den im jeweiligen transparenten EF gespeicherten Daten überein.

2.544 Testfall: READ BINARY ohne SFI (TC_READ_BINARY_WITHOUT_SFI_GF_1_2)

2.544.1 Informationen

ID	TC_READ_BINARY_WITHOUT_SFI_GF_1_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ BINARY ohne SFI erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für READ BINARY ohne SFI zum Auslesen eines transparenten EFs an das

	Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.544.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_01a, VI_02_12a

2.544.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- NO_CURRENT_EF- 2	Das EF ist ausgewählt
CN- WRONG_FILE_TYP E-2	Ausgewähltes EF ist transparent
CN- OFFSET_TOO_BIG- 2	Parameter "Offset" in Kommando-APDU ist nicht zu groß

2.544.4 APDU-Kommandos

ID: CM-READ_BINARY_WITHOUT_SFI_GF_1_2							
CLA	INS	P1	P2	Lc	Data	Le	
00	b0	XX	XX	--	--	XX	

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.544.5 Erwartete Ergebnisse

ID	Beschreibung
RS-31EA	XX...XX 90 00

2.544.6 Verifikationen

ID	Beschreibung
VF-READ_BINARY_WITHOUT_SFI-1	Die ausgelesenen Daten stimmen mit den im jeweiligen transparenten EF gespeicherten Daten überein.

2.545 Testfall: READ BINARY ohne SFI (TC_READ_BINARY_WITHOUT_SFI_GF_1_3)

2.545.1 Informationen

ID	TC_READ_BINARY_WITHOUT_SFI_GF_1_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ BINARY ohne SFI erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für READ BINARY ohne SFI zum Auslesen eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.545.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_01a, VI_02_12a

2.545.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_CURRENT_EF-2	Das EF ist ausgewählt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist transparent
CN-OFFSET_TOO_BIG-2	Parameter "Offset" in Kommando-APDU ist nicht zu groß

2.545.4 APDU-Kommandos

ID: CM-READ_BINARY_WITHOUT_SFI_GF_1_3						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.545.5 Erwartete Ergebnisse

ID	Beschreibung
RS-31EA	XX...XX 90 00

2.545.6 Verifikationen

ID	Beschreibung
VF-READ_BINARY_WITHOUT_SFI-1	Die ausgelesenen Daten stimmen mit den im jeweiligen transparenten EF gespeicherten Daten überein.

2.546 Testfall: READ BINARY ohne SFI (TC_READ_BINARY_WITHOUT_SFI_FF_1)

2.546.1 Informationen

ID	TC_READ_BINARY_WITHOUT_SFI_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ BINARY ohne SFI nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für READ BINARY ohne SFI zum Auslesen eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.546.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_01a, VI_02_12a

2.546.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"

CN- NO_CURRENT_EF- 2	Das EF ist ausgewählt
CN- WRONG_FILE_TYP E-2	Ausgewähltes EF ist transparent
CN- OFFSET_TOO_BIG- 2	Parameter "Offset" in Kommando-APDU ist nicht zu groß

2.546.4 APDU-Kommandos

ID: CM-READ_BINARY_WITHOUT_SFI_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.546.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.546.6 Verifikationen

ID	Beschreibung
VF-READ_BINARY_WITHOUT_SFI-2	Die ausgelesenen Daten stimmen nicht mit den im jeweiligen transparenten EF gespeicherten Daten überein.

2.547 Testfall: READ BINARY ohne SFI (TC_READ_BINARY_WITHOUT_SFI_FF_2)

2.547.1 Informationen

ID	TC_READ_BINARY_WITHOUT_SFI_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ BINARY ohne SFI nicht erfolgreich durchgeführt werden kann, wenn kein EF selektiert ist. Dazu wird eine Kommandonachricht für READ BINARY ohne SFI zum Auslesen eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.547.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_01a, VI_02_12a

2.547.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-NO_CURRENT_EF-1	Das EF ist nicht ausgewählt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist transparent

CN-OFFSET_TOO_BIG-2	Parameter "Offset" in Kommando-APDU ist nicht zu groß

2.547.4 APDU-Kommandos

ID: CM-READ_BINARY_WITHOUT_SFI_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.547.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6986	Das Testsystem antwortet mit '69 86'.

2.547.6 Verifikationen

ID	Beschreibung
VF-READ_BINARY_WITHOUT_SFI-2	Die ausgelesenen Daten stimmen nicht mit den im jeweiligen transparenten EF gespeicherten Daten überein.

2.548 Testfall: READ BINARY ohne SFI (TC_READ_BINARY_WITHOUT_SFI_GF_1)

2.548.1 Informationen

ID	TC_READ_BINARY_WITHOUT_SFI_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ BINARY ohne SFI mit einem manipulierten Kryptogramm erfolgreich mit der entsprechenden Fehlermeldung abgebrochen wird. Die Durchführung erfolgt anhand eines beliebigen transparenten File, das keinen Lesezugriff zulässt. Dazu wird

	eine Kommandonachricht für READ BINARY ohne SFI zum Auslesen eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.548.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_01a, VI_02_12a

2.548.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-CURRENT_EF-2	Das EF ist ausgewählt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist transparent
CN-OFFSET_TOO_BIG-2	Parameter "Offset" in Kommando-APDU ist nicht zu groß

2.548.4 APDU-Kommandos

ID: CM-READ_BINARY_WITHOUT_SFI_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält $(\text{Offset} - P2) / 256$, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.548.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6300	Das Testsystem antwortet mit '63 00'.

2.548.6 Verifikationen

ID	Beschreibung
VF-READ_BINARY_WITHOUT_SFI-1	Die ausgelesenen Daten stimmen mit den im jeweiligen transparenten EF gespeicherten Daten überein.

2.549 Testfall: READ BINARY ohne SFI (TC_READ_BINARY_WITHOUT_SFI_FF_1)

2.549.1 Informationen

ID	TC_READ_BINARY_WITHOUT_SFI_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ BINARY ohne SFI nicht erfolgreich durchgeführt werden kann, wenn das ausgewählte EF nicht transparent ist. Dazu wird eine Kommandonachricht für READ BINARY ohne SFI zum Auslesen eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.549.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_01a, VI_02_12a

2.549.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-WRONG_FILE_TYPE-1	Ausgewähltes EF ist nicht transparent
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NOT_CURRENT_EFFECT-2	Das EF ist ausgewählt
CN-OFFSET_TOO_BIG-2	Parameter "Offset" in Kommando-APDU ist nicht zu groß

2.549.4 APDU-Kommandos

ID: CM-READ_BINARY_WITHOUT_SFI_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.549.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6981	Das Testsystem antwortet mit '69 81'.

2.549.6 Verifikationen

ID	Beschreibung
VF-READ_BINARY_WITHOUT_SFI-2	Die ausgelesenen Daten stimmen nicht mit den im jeweiligen transparenten EF gespeicherten Daten überein.

2.550 Testfall: READ BINARY ohne SFI (TC_READ_BINARY_WITHOUT_SFI_FF_2)

2.550.1 Informationen

ID	TC_READ_BINARY_WITHOUT_SFI_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ BINARY ohne SFI nicht erfolgreich durchgeführt werden kann, wenn der Parameter "Offset" in Kommando-APDU zu groß ist. Die Durchführung erfolgt für einen Offset, der über das File-Ende hinausgeht. Dazu wird eine Kommandonachricht für READ BINARY ohne SFI zum Auslesen eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.550.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_01a, VI_02_12a

2.550.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OFFSET_TOO_BIG-	Parameter "Offset" in Kommando-APDU ist zu groß

1	
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_CURRENT_EF-2	Das EF ist ausgewählt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist transparent

2.550.4 APDU-Kommandos

ID: CM-READ_BINARY_WITHOUT_SFI_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.550.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6B00	Das Testsystem antwortet mit '6b 00'.

2.550.6 Verifikationen

ID	Beschreibung
VF-READ_BINARY_WITHOUT_SFI-2	Die ausgelesenen Daten stimmen nicht mit den im jeweiligen transparenten EF gespeicherten Daten überein.

2.551 Testfall: READ BINARY mit SFI (TC_READ_BINARY_WITH_SFI_GF_1_1)

2.551.1 Informationen

ID	TC_READ_BINARY_WITH_SFI_GF_1_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ BINARY mit SFI erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für READ BINARY mit SFI zum Auslesen eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.551.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_01b, VI_02_12b

2.551.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- FILE_NOT_FOUND- 2	Das per SFI adressierte File kann gefunden werden
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

CN-WRONG_FILE_TYP E-2	Ausgewähltes EF ist transparent
CN-OFFSET_TOO_BIG- 2	Parameter "Offset" in Kommando-APDU ist nicht zu groß

2.551.4 APDU-Kommandos

ID: CM-READ_BINARY_WITH_SFI_GF_1_1						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält '80' + SFI.

'P2' enthält den Offset aus {'00', ..., 'FF'}.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.551.5 Erwartete Ergebnisse

ID	Beschreibung
RS-31EA	XX...XX 90 00

2.551.6 Verifikationen

ID	Beschreibung
VF-READ_BINARY_WITH_SFI-1	Die ausgelesenen Daten stimmen mit den im jeweiligen transparenten EF gespeicherten Daten überein.

2.552 Testfall: READ BINARY mit SFI (TC_READ_BINARY_WITH_SFI_GF_1_2)

2.552.1 Informationen

ID	TC_READ_BINARY_WITH_SFI_GF_1_2

Beschreibung	Dieser Test verifiziert, dass ein Kommando READ BINARY mit SFI erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für READ BINARY mit SFI zum Auslesen eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.552.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_01b, VI_02_12b

2.552.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist transparent
CN-OFFSET_TOO_BIG-2	Parameter "Offset" in Kommando-APDU ist nicht zu groß

2.552.4 APDU-Kommandos

ID: CM-READ_BINARY_WITH_SFI_GF_1_2						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält '80' + SFI.

'P2' enthält den Offset aus {'00', ..., 'FF'}.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.552.5 Erwartete Ergebnisse

ID	Beschreibung
RS-31EA	XX...XX 90 00

2.552.6 Verifikationen

ID	Beschreibung
VF-READ_BINARY_WITH_SFI-1	Die ausgelesenen Daten stimmen mit den im jeweiligen transparenten EF gespeicherten Daten überein.

2.553 Testfall: READ BINARY mit SFI (TC_READ_BINARY_WITH_SFI_GF_1_3)

2.553.1 Informationen

ID	TC_READ_BINARY_WITH_SFI_GF_1_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ BINARY mit SFI erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für READ BINARY mit SFI zum Auslesen eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.553.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_01b, VI_02_12b

2.553.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist transparent
CN-OFFSET_TOO_BIG-2	Parameter "Offset" in Kommando-APDU ist nicht zu groß

2.553.4 APDU-Kommandos

ID: CM-READ_BINARY_WITH_SFI_GF_1_3						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält '80' + SFI.

'P2' enthält den Offset aus {'00', ..., 'FF'}.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.553.5 Erwartete Ergebnisse

ID	Beschreibung
RS-31EA	XX...XX 90 00

2.553.6 Verifikationen

ID	Beschreibung
VF-READ_BINARY_WITH_SFI-1	Die ausgelesenen Daten stimmen mit den im jeweiligen transparenten EF gespeicherten Daten überein.

2.554 Testfall: READ BINARY mit SFI (TC_READ_BINARY_WITH_SFI_FF_1)

2.554.1 Informationen

ID	TC_READ_BINARY_WITH_SFI_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ BINARY mit SFI nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für READ BINARY mit SFI zum Auslesen eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.554.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_01b, VI_02_12b

2.554.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist transparent
CN-OFFSET_TOO_BIG-2	Parameter "Offset" in Kommando-APDU ist nicht zu groß

2.554.4 APDU-Kommandos

ID: CM-READ_BINARY_WITH_SFI_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält '80' + SFI.

'P2' enthält den Offset aus {'00', ..., 'FF'}.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.554.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.554.6 Verifikationen

ID	Beschreibung
VF-READ_BINARY_WITH_SFI-2	Die ausgelesenen Daten stimmen nicht mit den im jeweiligen transparenten EF gespeicherten Daten überein.

2.555 Testfall: READ BINARY mit SFI (TC_READ_BINARY_WITH_SFI_FF_2)

2.555.1 Informationen

ID	TC_READ_BINARY_WITH_SFI_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ BINARY mit SFI nicht erfolgreich durchgeführt werden kann, wenn das per SFI adressierte File nicht gefunden werden kann. Dazu wird eine Kommandonachricht für READ BINARY mit SFI zum Auslesen eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.555.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_01b, VI_02_12b

2.555.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-FILE_NOT_FOUND-1	Das per SFI adressierte File kann nicht gefunden werden

CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist transparent
CN-OFFSET_TOO_BIG-2	Parameter "Offset" in Kommando-APDU ist nicht zu groß

2.555.4 APDU-Kommandos

ID: CM-READ_BINARY_WITH_SFI_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält '80' + SFI.

'P2' enthält den Offset aus {'00', ..., 'FF'}.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.555.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A82	Das Testsystem antwortet mit '6a 82'.

2.555.6 Verifikationen

ID	Beschreibung
VF-READ_BINARY_WITH_SFI-2	Die ausgelesenen Daten stimmen nicht mit den im jeweiligen transparenten EF gespeicherten Daten überein.

2.556 Testfall: READ BINARY mit SFI (TC_READ_BINARY_WITH_SFI_FF_3)

2.556.1 Informationen

ID	TC_READ_BINARY_WITH_SFI_FF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ BINARY mit SFI nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Dazu wird eine Kommandonachricht für READ BINARY mit SFI zum Auslesen eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.556.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_01b, VI_02_12b

2.556.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden

CN-WRONG_FILE_TYP E-2	Ausgewähltes EF ist transparent
CN-OFFSET_TOO_BIG- 2	Parameter "Offset" in Kommando-APDU ist nicht zu groß

2.556.4 APDU-Kommandos

ID: CM-READ_BINARY_WITH_SFI_FF_3						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält '80' + SFI.

'P2' enthält den Offset aus {'00', ..., 'FF'}.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.556.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.556.6 Verifikationen

ID	Beschreibung
VF-READ_BINARY_WITH_SFI-2	Die ausgelesenen Daten stimmen nicht mit den im jeweiligen transparenten EF gespeicherten Daten überein.

2.557 Testfall: READ BINARY mit SFI (TC_READ_BINARY_WITH_SFI_FF_4)

2.557.1 Informationen

ID	TC_READ_BINARY_WITH_SFI_FF_4

Beschreibung	Dieser Test verifiziert, dass ein Kommando READ BINARY mit SFI nicht erfolgreich durchgeführt werden kann, wenn das ausgewählte EF nicht transparent ist. Dazu wird eine Kommandonachricht für READ BINARY mit SFI zum Auslesen eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.557.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_01b, VI_02_12b

2.557.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-WRONG_FILE_TYPE-1	Ausgewähltes EF ist nicht transparent
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-OFFSET_TOO_BIG-2	Parameter "Offset" in Kommando-APDU ist nicht zu groß

2.557.4 APDU-Kommandos

ID: CM-READ_BINARY_WITH_SFI_FF_4						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält '80' + SFI.

'P2' enthält den Offset aus {'00', ..., 'FF'}.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.557.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6981	Das Testsystem antwortet mit '69 81'.

2.557.6 Verifikationen

ID	Beschreibung
VF-READ_BINARY_WITH_SFI-2	Die ausgelesenen Daten stimmen nicht mit den im jeweiligen transparenten EF gespeicherten Daten überein.

2.558 Testfall: READ BINARY mit SFI (TC_READ_BINARY_WITH_SFI_FF_5)

2.558.1 Informationen

ID	TC_READ_BINARY_WITH_SFI_FF_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ BINARY mit SFI nicht erfolgreich durchgeführt werden kann, wenn der Parameter "Offset" in Kommando-APDU zu groß ist. Dazu wird eine Kommandonachricht für READ BINARY mit SFI zum Auslesen eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.558.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_01b, VI_02_12b

2.558.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OFFSET_TOO_BIG-1	Parameter "Offset" in Kommando-APDU ist zu groß
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden
CN-SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist transparent

2.558.4 APDU-Kommandos

ID: CM-READ_BINARY_WITH_SFI_FF_5						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält '80' + SFI.

'P2' enthält den Offset aus {'00', ..., 'FF'}.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.558.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6B00	Das Testsystem antwortet mit '6b 00'.

2.558.6 Verifikationen

ID	Beschreibung
VF-READ_BINARY_WITH_SFI-2	Die ausgelesenen Daten stimmen nicht mit den im jeweiligen transparenten EF gespeicherten Daten überein.

2.559 Testfall: READ RECORD ohne SFI (TC_READ_RECORD_WITHOUT_SFI_GF_1)

2.559.1 Informationen

ID	TC_READ_RECORD_WITHOUT_SFI_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ RECORD ohne SFI erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für READ RECORD ohne SFI zum Auslesen eines record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.559.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_02a, PN_03_04a, VI_02_13a

2.559.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_CURRENT_EF-2	Das EF ist ausgewählt
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist strukturiert
CN-RECORD_NOT_FOUND-2	Record-Nummer existiert

2.559.4 APDU-Kommandos

ID: CM-READ_RECORD_WITHOUT_SFI_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.559.5 Erwartete Ergebnisse

ID	Beschreibung
RS-31EA	XX...XX 90 00

2.559.6 Verifikationen

ID	Beschreibung
VF-READ_RECORD_WITHOUT_SFI-1	Die ausgelesenen Daten stimmen mit den im jeweiligen record-orientierten EF gespeicherten Daten überein.

2.560 Testfall: READ RECORD ohne SFI (TC_READ_RECORD_WITHOUT_SFI_FF_1)

2.560.1 Informationen

ID	TC_READ_RECORD_WITHOUT_SFI_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ RECORD ohne SFI nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für READ RECORD ohne SFI zum Auslesen eines record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.560.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_02a, PN_03_04a, VI_02_13a

2.560.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"

CN- NO_CURRENT_EF- 2	Das EF ist ausgewählt
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN- WRONG_FILE_TYP E-2	Ausgewähltes EF ist strukturiert
CN- RECORD_NOT_FO UND-2	Record-Nummer existiert

2.560.4 APDU-Kommandos

ID: CM-READ_RECORD_WITHOUT_SFI_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Nummer.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.560.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.560.6 Verifikationen

ID	Beschreibung
VF-READ_RECORD_WITHOUT_SFI-2	Die ausgelesenen Daten stimmen nicht mit den im jeweiligen record-orientierten EF gespeicherten Daten überein.

2.561 Testfall: READ RECORD ohne SFI (TC_READ_RECORD_WITHOUT_SFI_FF_2)

2.561.1 Informationen

ID	TC_READ_RECORD_WITHOUT_SFI_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ RECORD ohne SFI nicht erfolgreich durchgeführt werden kann, wenn kein EF selektiert ist. Dazu wird eine Kommandonachricht für READ RECORD ohne SFI zum Auslesen eines record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.561.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_02a, PN_03_04a, VI_02_13a

2.561.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- NO_CURRENT_EF- 1	Das EF ist nicht ausgewählt
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

CN-WRONG_FILE_TYP E-2	Ausgewähltes EF ist strukturiert
CN-RECORD_NOT_FO UND-2	Record-Nummer existiert

2.561.4 APDU-Kommandos

ID: CM-READ_RECORD_WITHOUT_SFI_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Nummer.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.561.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6986	Das Testsystem antwortet mit '69 86'.

2.561.6 Verifikationen

ID	Beschreibung
VF-READ_RECORD_WITHOUT_SFI-2	Die ausgelesenen Daten stimmen nicht mit den im jeweiligen record-orientierten EF gespeicherten Daten überein.

2.562 Testfall: READ RECORD ohne SFI (TC_READ_RECORD_WITHOUT_SFI_FF_3)

2.562.1 Informationen

ID	TC_READ_RECORD_WITHOUT_SFI_FF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ RECORD ohne SFI

	nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Dazu wird eine Kommandonachricht für READ RECORD ohne SFI zum Auslesen eines record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.562.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_02a, PN_03_04a, VI_02_13a

2.562.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-CURRENT_EF-2	Das EF ist ausgewählt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist strukturiert
CN-RECORD_NOT_FOUND-2	Record-Nummer existiert

2.562.4 APDU-Kommandos

ID: CM-READ_RECORD_WITHOUT_SFI_FF_3						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.562.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.562.6 Verifikationen

ID	Beschreibung
VF-READ_RECORD_WITHOUT_SFI-2	Die ausgelesenen Daten stimmen nicht mit den im jeweiligen record-orientierten EF gespeicherten Daten überein.

2.563 Testfall: READ RECORD ohne SFI (TC_READ_RECORD_WITHOUT_SFI_FF_4)

2.563.1 Informationen

ID	TC_READ_RECORD_WITHOUT_SFI_FF_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ RECORD ohne SFI nicht erfolgreich durchgeführt werden kann, wenn das ausgewählte EF keine Record-basierte Struktur aufweist. Dazu wird eine Kommandonachricht für READ RECORD ohne SFI zum Auslesen eines record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.563.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_02a, PN_03_04a, VI_02_13a

2.563.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-WRONG_FILE_TYPE-1	Ausgewähltes EF ist nicht strukturiert
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NOT_CURRENT_EF-2	Das EF ist ausgewählt
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-RECORD_NOT_FOUND-2	Record-Nummer existiert

2.563.4 APDU-Kommandos

ID: CM-READ_RECORD_WITHOUT_SFI_FF_4						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.563.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6981	Das Testsystem antwortet mit '69 81'.

2.563.6 Verifikationen

ID	Beschreibung
VF-READ_RECORD_WITHOUT_SFI-2	Die ausgelesenen Daten stimmen nicht mit den im jeweiligen record-orientierten EF gespeicherten Daten überein.

2.564 Testfall: READ RECORD ohne SFI (TC_READ_RECORD_WITHOUT_SFI_FF_5)

2.564.1 Informationen

ID	TC_READ_RECORD_WITHOUT_SFI_FF_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ RECORD ohne SFI nicht erfolgreich durchgeführt werden kann, wenn die Record-Nummer nicht existiert. Dazu wird eine Kommandonachricht für READ RECORD ohne SFI zum Auslesen eines record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.564.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_02a, PN_03_04a, VI_02_13a

2.564.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- RECORD_NOT_FO UND-1	Record-Nummer existiert nicht
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- NO_CURRENT_EF- 2	Das EF ist ausgewählt
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN- WRONG_FILE_TYP E-2	Ausgewähltes EF ist strukturiert

2.564.4 APDU-Kommandos

ID: CM-READ_RECORD_WITHOUT_SFI_FF_5						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.564.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A83	Das Testsystem antwortet mit '6a 83'.

2.564.6 Verifikationen

ID	Beschreibung

VF-READ_RECORD_WITHOUT_SFI-2	Die ausgelesenen Daten stimmen nicht mit den im jeweiligen record-orientierten EF gespeicherten Daten überein.

2.565 Testfall: READ RECORD mit SFI (TC_READ_RECORD_WITH_SFI_GF_1)

2.565.1 Informationen

ID	TC_READ_RECORD_WITH_SFI_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ RECORD mit SFI erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für READ RECORD mit SFI zum Auslesen eines record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.565.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_02b, PN_03_04b, VI_02_13b

2.565.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN- WRONG_FILE_TYP E-2	Ausgewähltes EF ist strukturiert
CN- RECORD_NOT_FO UND-2	Record-Nummer existiert

2.565.4 APDU-Kommandos

ID: CM-READ_RECORD_WITH_SFI_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	XX	--	--	XX

'P1' enthält die Record-Number.

'P2' enthält (SFI << 3) + '04' (Read Record der Nummer wie in P1 angegeben).

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.565.5 Erwartete Ergebnisse

ID	Beschreibung
RS-31EA	XX...XX 90 00

2.565.6 Verifikationen

ID	Beschreibung
VF-READ_RECORD_WITH_SFI-1	Die ausgelesenen Daten stimmen mit den im jeweiligen record-orientierten EF gespeicherten Daten überein.

2.566 Testfall: READ RECORD mit SFI (TC_READ_RECORD_WITH_SFI_FF_1)

2.566.1 Informationen

ID	TC_READ_RECORD_WITH_SFI_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ RECORD mit SFI nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für READ RECORD mit SFI zum Auslesen eines record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.566.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_02b, PN_03_04b, VI_02_13b

2.566.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

CN-WRONG_FILE_TYP E-2	Ausgewähltes EF ist strukturiert
CN-RECORD_NOT_FO UND-2	Record-Nummer existiert

2.566.4 APDU-Kommandos

ID: CM-READ_RECORD_WITH_SFI_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	XX	--	--	XX

'P1' enthält die Record-Nummer.

'P2' enthält (SFI << 3) + '04' (Read Record der Nummer wie in P1 angegeben).

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.566.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.566.6 Verifikationen

ID	Beschreibung
VF-READ_RECORD_WITH_SFI-2	Die ausgelesenen Daten stimmen nicht mit den im jeweiligen record-orientierten EF gespeicherten Daten überein.

2.567 Testfall: READ RECORD mit SFI (TC_READ_RECORD_WITH_SFI_FF_2)

2.567.1 Informationen

ID	TC_READ_RECORD_WITH_SFI_FF_2

Beschreibung	Dieser Test verifiziert, dass ein Kommando READ RECORD mit SFI nicht erfolgreich durchgeführt werden kann, wenn das per SFI adressierte File nicht gefunden werden kann. Dazu wird eine Kommandonachricht für READ RECORD mit SFI zum Auslesen eines record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.567.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_02b, PN_03_04b, VI_02_13b

2.567.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-FILE_NOT_FOUND-1	Das per SFI adressierte File kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist strukturiert
CN-RECORD_NOT_FOUND-2	Record-Nummer existiert

2.567.4 APDU-Kommandos

ID: CM-READ_RECORD_WITH_SFI_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	XX	--	--	XX

'P1' enthält die Record-Number.

'P2' enthält (SFI << 3) + '04' (Read Record der Nummer wie in P1 angegeben).

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.567.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A82	Das Testsystem antwortet mit '6a 82'.

2.567.6 Verifikationen

ID	Beschreibung
VF-READ_RECORD_WITH_SFI-2	Die ausgelesenen Daten stimmen nicht mit den im jeweiligen record-orientierten EF gespeicherten Daten überein.

2.568 Testfall: READ RECORD mit SFI (TC_READ_RECORD_WITH_SFI_FF_3)

2.568.1 Informationen

ID	TC_READ_RECORD_WITH_SFI_FF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ RECORD mit SFI nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Dazu wird eine Kommandonachricht für READ RECORD mit SFI zum Auslesen eines record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.568.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_02b, PN_03_04b, VI_02_13b

2.568.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist strukturiert
CN-RECORD_NOT_FOUND-2	Record-Nummer existiert

2.568.4 APDU-Kommandos

ID: CM-READ_RECORD_WITH_SFI_FF_3						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	XX	--	--	XX

'P1' enthält die Record-Nummer.

'P2' enthält (SFI << 3) + '04' (Read Record der Nummer wie in P1 angegeben).

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.568.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.568.6 Verifikationen

ID	Beschreibung
VF-READ_RECORD_WITH_SFI-2	Die ausgelesenen Daten stimmen nicht mit den im jeweiligen record-orientierten EF gespeicherten Daten überein.

2.569 Testfall: READ RECORD mit SFI (TC_READ_RECORD_WITH_SFI_FF_4)

2.569.1 Informationen

ID	TC_READ_RECORD_WITH_SFI_FF_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ RECORD mit SFI nicht erfolgreich durchgeführt werden kann, wenn das ausgewählte EF keine Record-basierte Struktur aufweist. Dazu wird eine Kommandonachricht für READ RECORD mit SFI zum Auslesen eines record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.569.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_02b, PN_03_04b, VI_02_13b

2.569.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-WRONG_FILE_TYPE-1	Ausgewähltes EF ist nicht strukturiert
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-RECORD_NOT_FOUND-2	Record-Nummer existiert

2.569.4 APDU-Kommandos

ID: CM-READ_RECORD_WITH_SFI_FF_4						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	XX	--	--	XX

'P1' enthält die Record-Nummer.

'P2' enthält (SFI << 3) + '04' (Read Record der Nummer wie in P1 angegeben).

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.569.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6981	Das Testsystem antwortet mit '69 81'.

2.569.6 Verifikationen

ID	Beschreibung
VF-READ_RECORD_WITH_SFI-2	Die ausgelesenen Daten stimmen nicht mit den im jeweiligen record-orientierten EF gespeicherten Daten überein.

2.570 Testfall: READ RECORD mit SFI (TC_READ_RECORD_WITH_SFI_FF_5)

2.570.1 Informationen

ID	TC_READ_RECORD_WITH_SFI_FF_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando READ RECORD mit SFI nicht erfolgreich durchgeführt werden kann, wenn die Record-Nummer nicht existiert. Dazu wird eine Kommandonachricht für READ RECORD mit SFI zum Auslesen eines record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.570.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.3

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_02b, PN_03_04b, VI_02_13b

2.570.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-RECORD_NOT_FOUND-1	Record-Nummer existiert nicht

CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist strukturiert

2.570.4 APDU-Kommandos

ID: CM-READ_RECORD_WITH_SFI_FF_5						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	XX	--	--	XX

'P1' enthält die Record-Number.

'P2' enthält (SFI << 3) + '04' (Read Record der Nummer wie in P1 angegeben).

'Le' enthält die Anzahl der zu erwartenden Oktette.

2.570.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A83	Das Testsystem antwortet mit '6a 83'.

2.570.6 Verifikationen

ID	Beschreibung
VF-READ_RECORD_WITH_SFI-2	Die ausgelesenen Daten stimmen nicht mit den im jeweiligen record-orientierten EF gespeicherten Daten überein.

2.571 Testfall: SELECT eines DF mittels AID (TC_SELECT_DF_AID_GF_1_1)

2.571.1 Informationen

ID	TC_SELECT_DF_AID_GF_1_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando SELECT eines DF mittels AID erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für SELECT eines DF mittels AID zur Auswahl eines DFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.571.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_16d

2.571.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das zu selektierende File kann gefunden werden

2.571.4 APDU-Kommandos

ID: CM-SELECT_DF_AID_GF_1_1

CLA	INS	P1	P2	Lc	Data	Le
00	a4	04	0c	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Application-Identifizierer des zu selektierenden DF.

2.571.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.571.6 Verifikationen

ID	Beschreibung
VF-SELECT_DF_AID-1	Nachfolgende, vom SELECT-Kommando abhängige Kommandos, werden vom SM nicht mit einer SELECT-bezogenen Fehlermeldung beantwortet.

2.572 Testfall: SELECT eines DF mittels AID (TC_SELECT_DF_AID_GF_1_2)

2.572.1 Informationen

ID	TC_SELECT_DF_AID_GF_1_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando SELECT eines DF mittels AID erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für SELECT eines DF mittels AID zur Auswahl eines DFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.572.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_16d

2.572.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das zu selektierende File kann gefunden werden

2.572.4 APDU-Kommandos

ID: CM-SELECT_DF_AID_GF_1_2						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	04	0c	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Application-Identifizier des zu selektierenden DF.

2.572.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.572.6 Verifikationen

ID	Beschreibung
VF-SELECT_DF_AID-1	Nachfolgende, vom SELECT-Kommando abhängige Kommandos, werden vom SM nicht mit einer SELECT-bezogenen Fehlermeldung beantwortet.

2.573 Testfall: SELECT eines DF mittels AID (TC_SELECT_DF_AID_GF_2_1)

2.573.1 Informationen

ID	TC_SELECT_DF_AID_GF_2_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando SELECT eines DF mittels AID nicht erfolgreich durchgeführt werden kann, wenn das ausgewählte FILE logisch/physikalisch deaktiviert ist. Dazu wird eine Kommandonachricht für SELECT eines DF mittels AID zur Auswahl eines DFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.573.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_16d

2.573.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-FILE_DEACTIVATED-1	Ausgewähltes FILE ist logisch/physikalisch deaktiviert
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das zu selektierende File kann gefunden werden

2.573.4 APDU-Kommandos

ID: CM-SELECT_DF_AID_GF_2_1						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	04	0c	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Application-Identifizier des zu selektierenden DF.

2.573.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6283	Das Testsystem antwortet mit '62 83'.

2.573.6 Verifikationen

ID	Beschreibung
VF-SELECT_DF_AID-1	Nachfolgende, vom SELECT-Kommando abhängige Kommandos, werden vom SM nicht mit einer SELECT-bezogenen Fehlermeldung beantwortet.

2.574 Testfall: SELECT eines DF mittels AID (TC_SELECT_DF_AID_GF_2_2)

2.574.1 Informationen

ID	TC_SELECT_DF_AID_GF_2_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando SELECT eines DF mittels AID nicht erfolgreich durchgeführt werden kann, wenn das ausgewählte FILE logisch/physikalisch deaktiviert ist. Dazu wird eine Kommandonachricht für SELECT eines DF mittels AID zur Auswahl eines DFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.574.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_16d

2.574.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-FILE_DEACTIVATED-1	Ausgewähltes FILE ist logisch/physikalisch deaktiviert
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das zu selektierende File kann gefunden werden

2.574.4 APDU-Kommandos

ID: CM-SELECT_DF_AID_GF_2_2						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	04	0c	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Application-Identifier des zu selektierenden DF.

2.574.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6283	Das Testsystem antwortet mit '62 83'.

2.574.6 Verifikationen

ID	Beschreibung
VF-SELECT_DF_AID-1	Nachfolgende, vom SELECT-Kommando abhängige Kommandos, werden vom SM nicht mit einer SELECT-bezogenen Fehlermeldung beantwortet.

2.575 Testfall: SELECT eines DF mittels AID (TC_SELECT_DF_AID_GF_3)

2.575.1 Informationen

ID	TC_SELECT_DF_AID_GF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando SELECT eines DF mittels AID nicht erfolgreich durchgeführt werden kann, wenn das ausgewählte FILE logisch/physikalisch terminiert ist. Dazu wird eine Kommandonachricht für SELECT eines DF mittels AID zur Auswahl eines DFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.575.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_16d

2.575.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-FILE_TERMINATE	Ausgewähltes FILE ist logisch/physikalisch terminiert

D-1	
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das zu selektierende File kann gefunden werden

2.575.4 APDU-Kommandos

ID: CM-SELECT_DF_AID_GF_3						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	04	0c	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Application-Identifizier des zu selektierenden DF.

2.575.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6285	Das Testsystem antwortet mit '62 85'.

2.575.6 Verifikationen

ID	Beschreibung
VF-SELECT_DF_AID-1	Nachfolgende, vom SELECT-Kommando abhängige Kommandos, werden vom SM nicht mit einer SELECT-bezogenen Fehlermeldung beantwortet.

2.576 Testfall: SELECT eines DF mittels AID (TC_SELECT_DF_AID_FF_1)

2.576.1 Informationen

ID	TC_SELECT_DF_AID_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando SELECT eines DF mittels AID nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für SELECT eines DF mittels AID zur Auswahl eines DFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.576.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_16d

2.576.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- INSTRUCTION_NO T_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN- FILE_NOT_FOUND- 2	Das zu selektierende File kann gefunden werden

2.576.4 APDU-Kommandos

ID: CM-SELECT_DF_AID_FF_1

CLA	INS	P1	P2	Lc	Data	Le
00	a4	04	0c	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Application-Identifizier des zu selektierenden DF.

2.576.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.576.6 Verifikationen

ID	Beschreibung
VF-SELECT_DF_AID-2	Nachfolgende, vom SELECT-Kommando abhängige Kommandos, werden vom SM mit einer SELECT-bezogenen Fehlermeldung beantwortet.

2.577 Testfall: SELECT eines DF mittels AID (TC_SELECT_DF_AID_FF_2)

2.577.1 Informationen

ID	TC_SELECT_DF_AID_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando SELECT eines DF mittels AID nicht erfolgreich durchgeführt werden kann, wenn das zu selektierende File nicht gefunden werden kann. Dazu wird eine Kommandonachricht für SELECT eines DF mittels AID zur Auswahl eines DFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.577.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_16d

2.577.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-FILE_NOT_FOUND-1	Das zu selektierende File kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

2.577.4 APDU-Kommandos

ID: CM-SELECT_DF_AID_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	04	0c	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Application-Identifizier des zu selektierenden DF.

2.577.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A82	Das Testsystem antwortet mit '6a 82'.

2.577.6 Verifikationen

ID	Beschreibung
VF-SELECT_DF_AID-2	Nachfolgende, vom SELECT-Kommando abhängige Kommandos, werden vom SM mit einer SELECT-bezogenen Fehlermeldung beantwortet.

2.578 Testfall: SELECT eines DF mittels FID (TC_SELECT_DF_FID_GF_1)

2.578.1 Informationen

ID	TC_SELECT_DF_FID_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando SELECT eines DF mittels FID erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für SELECT eines DF mittels FID zur Auswahl eines DFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.578.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_01a, PN_04_16b, PN_04_18a, PN_04_19a, PN_04_20a, PN_04_21a, VI_02_01b, VI_02_01c, VI_02_01d, VI_02_02a

2.578.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das zu selektierende File kann gefunden werden

2.578.4 APDU-Kommandos

ID: CM-SELECT_DF_FID_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	XX...XX	--

'Data' enthält den File-Identifizier des zu selektierenden DF.

2.578.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.578.6 Verifikationen

ID	Beschreibung
VF-SELECT_DF_FID-1	Nachfolgende, vom SELECT-Kommando abhängige Kommandos, werden vom SM nicht mit einer SELECT-bezogenen Fehlermeldung beantwortet.

2.579 Testfall: SELECT eines DF mittels FID (TC_SELECT_DF_FID_GF_2)

2.579.1 Informationen

ID	TC_SELECT_DF_FID_GF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando SELECT eines DF mittels FID nicht erfolgreich durchgeführt werden kann, wenn das ausgewählte FILE logisch/physikalisch deaktiviert ist. Dazu wird eine Kommandonachricht für SELECT eines DF mittels FID zur Auswahl eines DFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.579.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_01a, PN_04_16b, PN_04_18a, PN_04_19a, PN_04_20a, PN_04_21a, VI_02_01b, VI_02_01c, VI_02_01d, VI_02_02a

2.579.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-FILE_DEACTIVATED-1	Ausgewähltes FILE ist logisch/physikalisch deaktiviert
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das zu selektierende File kann gefunden werden

2.579.4 APDU-Kommandos

ID: CM-SELECT_DF_FID_GF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	XX...XX	--

'Data' enthält den File-Identifizier des zu selektierenden DF.

2.579.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6283	Das Testsystem antwortet mit '62 83'.

2.579.6 Verifikationen

ID	Beschreibung
VF-SELECT_DF_FID-1	Nachfolgende, vom SELECT-Kommando abhängige Kommandos, werden vom SM nicht mit einer SELECT-bezogenen Fehlermeldung beantwortet.

2.580 Testfall: SELECT eines DF mittels FID (TC_SELECT_DF_FID_GF_3)

2.580.1 Informationen

ID	TC_SELECT_DF_FID_GF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando SELECT eines DF mittels FID nicht erfolgreich durchgeführt werden kann, wenn das ausgewählte FILE logisch/physikalisch terminiert ist. Dazu wird eine Kommandonachricht für SELECT eines DF mittels FID zur Auswahl eines DFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.580.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_01a, PN_04_16b, PN_04_18a, PN_04_19a, PN_04_20a, PN_04_21a, VI_02_01b, VI_02_01c, VI_02_01d, VI_02_02a

2.580.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-	Ausgewähltes FILE ist logisch/physikalisch terminiert

FILE_TERMINATE D-1	
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- FILE_NOT_FOUND- 2	Das zu selektierende File kann gefunden werden

2.580.4 APDU-Kommandos

ID: CM-SELECT_DF_FID_GF_3						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	XX...XX	--

'Data' enthält den File-Identifizier des zu selektierenden DF.

2.580.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6285	Das Testsystem antwortet mit '62 85'.

2.580.6 Verifikationen

ID	Beschreibung
VF-SELECT_DF_FID-1	Nachfolgende, vom SELECT-Kommando abhängige Kommandos, werden vom SM nicht mit einer SELECT-bezogenen Fehlermeldung beantwortet.

2.581 Testfall: SELECT eines DF mittels FID (TC_SELECT_DF_FID_FF_1)

2.581.1 Informationen

ID	TC_SELECT_DF_FID_FF_1

Beschreibung	Dieser Test verifiziert, dass ein Kommando SELECT eines DF mittels FID nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für SELECT eines DF mittels FID zur Auswahl eines DFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.581.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_01a, PN_04_16b, PN_04_18a, PN_04_19a, PN_04_20a, PN_04_21a, VI_02_01b, VI_02_01c, VI_02_01d, VI_02_02a

2.581.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das zu selektierende File kann gefunden werden

2.581.4 APDU-Kommandos

ID: CM-SELECT_DF_FID_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	XX...XX	--

'Data' enthält den File-Identifizier des zu selektierenden DF.

2.581.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.581.6 Verifikationen

ID	Beschreibung
VF-SELECT_DF_FID-2	Nachfolgende, vom SELECT-Kommando abhängige Kommandos, werden vom SM mit einer SELECT-bezogenen Fehlermeldung beantwortet.

2.582 Testfall: SELECT eines DF mittels FID (TC_SELECT_DF_FID_FF_2)

2.582.1 Informationen

ID	TC_SELECT_DF_FID_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando SELECT eines DF mittels FID nicht erfolgreich durchgeführt werden kann, wenn das zu selektierende File nicht gefunden werden kann. Dazu wird eine Kommandonachricht für SELECT eines DF mittels FID zur Auswahl eines DFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.582.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_01a, PN_04_16b, PN_04_18a, PN_04_19a, PN_04_20a, PN_04_21a, VI_02_01b, VI_02_01c, VI_02_01d, VI_02_02a

2.582.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-FILE_NOT_FOUND-1	Das zu selektierende File kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

2.582.4 APDU-Kommandos

ID: CM-SELECT_DF_FID_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	XX...XX	--

'Data' enthält den File-Identifizier des zu selektierenden DF.

2.582.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A82	Das Testsystem antwortet mit '6a 82'.

2.582.6 Verifikationen

ID	Beschreibung
VF-SELECT_DF_FID-2	Nachfolgende, vom SELECT-Kommando abhängige Kommandos, werden vom SM mit einer SELECT-bezogenen Fehlermeldung beantwortet.

2.583 Testfall: SELECT eines MF (TC_SELECT_DF_MF_GF_1)

2.583.1 Informationen

ID	TC_SELECT_DF_MF_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando SELECT eines MF erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für SELECT eines MF zur Auswahl des MF an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.583.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_16a, VI_02_01a

2.583.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

2.583.4 APDU-Kommandos

ID: CM-SELECT_DF_MF_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	00	0c	02	3f00	--

2.583.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.583.6 Verifikationen

ID	Beschreibung
VF-SELECT_DF_MF-1	Nachfolgende, vom SELECT-Kommando abhängige Kommandos, werden vom SM nicht mit einer SELECT-bezogenen Fehlermeldung beantwortet.

2.584 Testfall: SELECT eines MF (TC_SELECT_DF_MF_FF_1)

2.584.1 Informationen

ID	TC_SELECT_DF_MF_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando SELECT eines MF nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für SELECT eines MF zur Auswahl des MF an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.584.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_16a, VI_02_01a

2.584.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- INSTRUCTION_NO T_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"

2.584.4 APDU-Kommandos

ID: CM-SELECT_DF_MF_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	00	0c	02	3f00	--

2.584.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.584.6 Verifikationen

ID	Beschreibung
VF-SELECT_DF_MF-2	Nachfolgende, vom SELECT-Kommando abhängige Kommandos, werden vom SM mit einer SELECT-bezogenen Fehlermeldung beantwortet.

2.585 Testfall: SELECT eines EF mittels FID (TC_SELECT_EF_GF_1)

2.585.1 Informationen

ID	TC_SELECT_EF_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando SELECT eines EF mittels FID erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für

	SELECT eines EF zur Auswahl eines EFs an das Sicherheitsmodul gesendet Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.585.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_02a, PN_02_03a, PN_03_04a, PN_03_05a, PN_03_05b, PN_04_14a, PN_04_15a, PN_04_16c, VI_02_13a, VI_02_14a, VI_03_01a, VI_03_05a, VI_04_02a

2.585.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das zu selektierende File kann gefunden werden

2.585.4 APDU-Kommandos

ID: CM-SELECT_EF_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	02	0c	02	XX...XX	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

2.585.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.585.6 Verifikationen

ID	Beschreibung
VF-SELECT_EF_FID-1	Nachfolgende, vom SELECT-Kommando abhängige Kommandos, werden vom SM nicht mit einer SELECT-bezogenen Fehlermeldung, wie z. B. '69 86', beantwortet.

2.586 Testfall: SELECT eines EF mittels FID (TC_SELECT_EF_GF_2)

2.586.1 Informationen

ID	TC_SELECT_EF_GF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando SELECT eines EF mittels FID nicht erfolgreich durchgeführt werden kann, wenn das ausgewählte FILE logisch/physikalisch deaktiviert ist. Dazu wird eine Kommandonachricht für SELECT eines EF zur Auswahl eines EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.586.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_02a, PN_02_03a, PN_03_04a, PN_03_05a, PN_03_05b, PN_04_14a, PN_04_15a, PN_04_16c, VI_02_13a, VI_02_14a, VI_03_01a, VI_03_05a, VI_04_02a

2.586.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-FILE_DEACTIVATED-1	Ausgewähltes FILE ist logisch/physikalisch deaktiviert
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das zu selektierende File kann gefunden werden

2.586.4 APDU-Kommandos

ID: CM-SELECT_EF_GF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	02	0c	02	XX...XX	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

2.586.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6283	Das Testsystem antwortet mit '62 83'.

2.586.6 Verifikationen

ID	Beschreibung
VF-SELECT_EF_FID-1	Nachfolgende, vom SELECT-Kommando abhängige Kommandos, werden vom SM nicht mit einer SELECT-bezogenen Fehlermeldung, wie z. B. '69 86', beantwortet.

2.587 Testfall: SELECT eines EF mittels FID (TC_SELECT_EF_GF_3)

2.587.1 Informationen

ID	TC_SELECT_EF_GF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando SELECT eines EF mittels FID nicht erfolgreich durchgeführt werden kann, wenn das ausgewählte FILE logisch/physikalisch terminiert ist. Dazu wird eine Kommandonachricht für SELECT eines EF zur Auswahl eines EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.587.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_02a, PN_02_03a, PN_03_04a, PN_03_05a, PN_03_05b, PN_04_14a, PN_04_15a, PN_04_16c, VI_02_13a, VI_02_14a, VI_03_01a, VI_03_05a, VI_04_02a

2.587.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-FILE_TERMINATED-1	Ausgewähltes FILE ist logisch/physikalisch terminiert
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-	Das zu selektierende File kann gefunden werden

2.587.4 APDU-Kommandos

ID: CM-SELECT_EF_GF_3						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	02	0c	02	XX...XX	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

2.587.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6285	Das Testsystem antwortet mit '62 85'.

2.587.6 Verifikationen

ID	Beschreibung
VF-SELECT_EF_FID-1	Nachfolgende, vom SELECT-Kommando abhängige Kommandos, werden vom SM nicht mit einer SELECT-bezogenen Fehlermeldung, wie z. B. '69 86', beantwortet.

2.588 Testfall: SELECT eines EF mittels FID (TC_SELECT_EF_FF_1)

2.588.1 Informationen

ID	TC_SELECT_EF_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando SELECT eines EF mittels FID nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für SELECT eines EF zur Auswahl eines EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.

Klassifizierung	Fehlerfall-Test

2.588.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_02a, PN_02_03a, PN_03_04a, PN_03_05a, PN_03_05b, PN_04_14a, PN_04_15a, PN_04_16c, VI_02_13a, VI_02_14a, VI_03_01a, VI_03_05a, VI_04_02a

2.588.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das zu selektierende File kann gefunden werden

2.588.4 APDU-Kommandos

ID: CM-SELECT_EF_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	02	0c	02	XX...XX	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

2.588.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.588.6 Verifikationen

ID	Beschreibung
VF-SELECT_EF_FID-2	Nachfolgende, vom SELECT-Kommando abhängige Kommandos, werden vom SM mit einer SELECT-bezogenen Fehlermeldung, wie z. B. '69 86', beantwortet.

2.589 Testfall: SELECT eines EF mittels FID (TC_SELECT_EF_FF_2)

2.589.1 Informationen

ID	TC_SELECT_EF_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando SELECT eines EF mittels FID nicht erfolgreich durchgeführt werden kann, wenn das zu selektierende File nicht gefunden werden kann. Dazu wird eine Kommandonachricht für SELECT eines EF zur Auswahl eines EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.589.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_02a, PN_02_03a, PN_03_04a, PN_03_05a, PN_03_05b, PN_04_14a, PN_04_15a, PN_04_16c, VI_02_13a, VI_02_14a, VI_03_01a, VI_03_05a, VI_04_02a

2.589.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN- FILE_NOT_FOUND-1	Das zu selektierende File kann nicht gefunden werden
CN- INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

2.589.4 APDU-Kommandos

ID: CM-SELECT_EF_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	02	0c	02	XX...XX	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

2.589.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A82	Das Testsystem antwortet mit '6a 82'.

2.589.6 Verifikationen

ID	Beschreibung
VF-SELECT_EF_FID-2	Nachfolgende, vom SELECT-Kommando abhängige Kommandos, werden vom SM mit einer SELECT-bezogenen Fehlermeldung, wie z. B. '69 86', beantwortet.

2.590 Testfall: TERMINATE CARD USAGE (TC_TERMINATE_CARD_USAGE_GF_1)

2.590.1 Informationen

ID	TC_TERMINATE_CARD_USAGE_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando TERMINATE CARD USAGE erfolgreich durchgeführt werden kann, sofern alle notwendigen

	Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für TERMINATE CARD USAGE zur Außerbetriebnahme des Sicherheitsmoduls an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.590.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.9.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_22

2.590.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.590.4 APDU-Kommandos

ID: CM-TERMINATE_CARD_USAGE_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	fe	00	00	--	--	--

2.590.5 Erwartete Ergebnisse

ID	Beschreibung

RS-9000	Das Testsystem antwortet mit '90 00'.

2.590.6 Verifikationen

ID	Beschreibung
VF-TERMINATE_CARD_USAGE-1	Das SM gibt nach dem Hochfahren bzw. nach einem Reset den ATR/ATS aus.
VF-TERMINATE_CARD_USAGE-2	Nachfolgende Kommandos werden vom SM mit '6d 00' beantwortet.

2.591 Testfall: TERMINATE CARD USAGE (TC_TERMINATE_CARD_USAGE_FF_1)

2.591.1 Informationen

ID	TC_TERMINATE_CARD_USAGE_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando TERMINATE CARD USAGE nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für TERMINATE CARD USAGE zur Außerbetriebnahme des Sicherheitsmoduls an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.591.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.9.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_22

2.591.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft

SEMANTIC_CORRECTNESS	(soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.591.4 APDU-Kommandos

ID: CM-TERMINATE_CARD_USAGE_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	fe	00	00	--	--	--

2.591.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.591.6 Verifikationen

ID	Beschreibung
VF-TERMINATE_CARD_USAGE-3	nachfolgende Kommandos werden vom SM nicht mit '6d 00' beantwortet.

2.592 Testfall: TERMINATE CARD USAGE (TC_TERMINATE_CARD_USAGE_FF_2)

2.592.1 Informationen

ID	TC_TERMINATE_CARD_USAGE_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando TERMINATE CARD USAGE

	nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Dazu wird eine Kommandonachricht für TERMINATE CARD USAGE zur Außerbetriebnahme des Sicherheitsmoduls an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.592.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.9.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_22

2.592.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

2.592.4 APDU-Kommandos

ID: CM-TERMINATE_CARD_USAGE_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	fe	00	00	--	--	--

2.592.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.592.6 Verifikationen

ID	Beschreibung
VF-TERMINATE_CARD_USAGE-3	nachfolgende Kommandos werden vom SM nicht mit '6d 00' beantwortet.

2.593 Testfall: TERMINATE DF (TC_TERMINATE_DF_GF_1)

2.593.1 Informationen

ID	TC_TERMINATE_DF_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando TERMINATE DF erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für TERMINATE DF zur Terminierung eines DFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.593.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_21a

2.593.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_CURRENT_FILE-2	Das File ist ausgewählt
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.593.4 APDU-Kommandos

ID: CM-TERMINATE_DF_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

2.593.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.593.6 Verifikationen

ID	Beschreibung
VF-TERMINATE_DF-1	Das nachfolgende Auswählen des entsprechenden DF ergibt 'file terminated'.

2.594 Testfall: TERMINATE DF (TC_TERMINATE_DF_FF_1)

2.594.1 Informationen

ID	TC_TERMINATE_DF_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando TERMINATE DF nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im

	Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für TERMINATE DF zur Terminierung eines DFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.594.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_21a

2.594.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-CURRENT_FILE-2	Das File ist ausgewählt
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.594.4 APDU-Kommandos

ID: CM-TERMINATE_DF_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

2.594.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.594.6 Verifikationen

ID	Beschreibung
VF-TERMINATE_DF-2	Das nachfolgende Auswählen des entsprechenden DF ergibt nicht 'file terminated'.

2.595 Testfall: TERMINATE DF (TC_TERMINATE_DF_FF_2)

2.595.1 Informationen

ID	TC_TERMINATE_DF_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando TERMINATE DF nicht durchführen lässt, wenn das File vorher nicht selektiert wurde. Dazu wird eine Kommandonachricht für TERMINATE DF zur Terminierung eines DFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.595.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_21a

2.595.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN- NO_CURRENT_FILE-1	Das File ist nicht ausgewählt
CN- INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.595.4 APDU-Kommandos

ID: CM-TERMINATE_DF_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

2.595.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6986	Das Testsystem antwortet mit '69 86'.

2.595.6 Verifikationen

ID	Beschreibung
VF-TERMINATE_DF-2	Das nachfolgende Auswählen des entsprechenden DF ergibt nicht 'file terminated'.

2.596 Testfall: TERMINATE DF (TC_TERMINATE_DF_FF_3)

2.596.1 Informationen

ID	TC_TERMINATE_DF_FF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando TERMINATE DF nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext

	des Objekts nicht erfüllt sind. Dazu wird eine Kommandonachricht für TERMINATE DF zur Terminierung eines DFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.596.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.6

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_21a

2.596.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_CURRENT_FILE-2	Das File ist ausgewählt

2.596.4 APDU-Kommandos

ID: CM-TERMINATE_DF_FF_3						
CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

2.596.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.596.6 Verifikationen

ID	Beschreibung
VF-TERMINATE_DF-2	Das nachfolgende Auswählen des entsprechenden DF ergibt nicht 'file terminated'.

2.597 Testfall: TERMINATE EF (TC_TERMINATE_EF_GF_1)

2.597.1 Informationen

ID	TC_TERMINATE_EF_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando TERMINATE EF erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für TERMINATE EF zur Terminierung eines EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.597.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.7

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_21b

2.597.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_CURRENT_FILE-2	Das File ist ausgewählt
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.597.4 APDU-Kommandos

ID: CM-TERMINATE_EF_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

2.597.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.597.6 Verifikationen

ID	Beschreibung
VF-TERMINATE_EF-1	Das nachfolgende Auswählen des entsprechenden EF ergibt 'file terminated'.

2.598 Testfall: TERMINATE EF (TC_TERMINATE_EF_FF_1)

2.598.1 Informationen

ID	TC_TERMINATE_EF_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando TERMINATE EF nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im

	Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für TERMINATE EF zur Terminierung eines EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.598.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.7

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_21b

2.598.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-CURRENT_FILE-2	Das File ist ausgewählt
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.598.4 APDU-Kommandos

ID: CM-TERMINATE_EF_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

2.598.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.598.6 Verifikationen

ID	Beschreibung
VF-TERMINATE_EF-2	Das nachfolgende Auswählen des entsprechenden EF ergibt nicht 'file terminated'.

2.599 Testfall: TERMINATE EF (TC_TERMINATE_EF_FF_2)

2.599.1 Informationen

ID	TC_TERMINATE_EF_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando TERMINATE EF nicht durchführen lässt, wenn das File vorher nicht selektiert wurde. Dazu wird eine Kommandonachricht für TERMINATE EF zur Terminierung eines EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.599.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.7

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_21b

2.599.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN- NO_CURRENT_FILE-1	Das File ist nicht ausgewählt
CN- INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- SECURITY_STATUS_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

2.599.4 APDU-Kommandos

ID: CM-TERMINATE_EF_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

2.599.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6986	Das Testsystem antwortet mit '69 86'.

2.599.6 Verifikationen

ID	Beschreibung
VF-TERMINATE_EF-2	Das nachfolgende Auswählen des entsprechenden EF ergibt nicht 'file terminated'.

2.600 Testfall: TERMINATE EF (TC_TERMINATE_EF_FF_3)

2.600.1 Informationen

ID	TC_TERMINATE_EF_FF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando TERMINATE EF nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext

	des Objekts nicht erfüllt sind. Dazu wird eine Kommandonachricht für TERMINATE EF zur Terminierung eines EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.600.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.2.7

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_21b

2.600.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_CURRENT_FILE-2	Das File ist ausgewählt

2.600.4 APDU-Kommandos

ID: CM-TERMINATE_EF_FF_3						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

2.600.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.600.6 Verifikationen

ID	Beschreibung
VF-TERMINATE_EF-2	Das nachfolgende Auswählen des entsprechenden EF ergibt nicht 'file terminated'.

2.601 Testfall: UPDATE BINARY ohne SFI (TC_UPDATE_BINARY_WITHOUT_SFI_GF_1)

2.601.1 Informationen

ID	TC_UPDATE_BINARY_WITHOUT_SFI_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE BINARY ohne SFI erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für UPDATE BINARY ohne SFI zum Schreiben oder Aktualisieren eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.601.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_14a, VI_03_01a, VI_03_05a

2.601.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft

SEMANTIC_CORRECTNESS	(soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_CURRENT_EF-2	Das EF ist ausgewählt
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist transparent
CN-OFFSET_TOO_BIG-2	Parameter "Offset" in Kommando-APDU ist nicht zu groß
CN-DATA_TOO_BIG-2	Parameter "neue Daten" ragt nicht über das Dateende hinaus

2.601.4 APDU-Kommandos

ID: CM-UPDATE_BINARY_WITHOUT_SFI_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.601.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.601.6 Verifikationen

ID	Beschreibung
VF-UPDATE_BINARY_WITHOUT_SFI-1	Der ausgelesene Inhalt des entsprechenden EF stimmt mit dem entsprechenden Inhalt dieses Testfalls überein

2.602 Testfall: UPDATE BINARY ohne SFI (TC_UPDATE_BINARY_WITHOUT_SFI_FF_1)

2.602.1 Informationen

ID	TC_UPDATE_BINARY_WITHOUT_SFI_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE BINARY ohne SFI nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für UPDATE BINARY ohne SFI zum Schreiben oder Aktualisieren eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.602.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_14a, VI_03_01a, VI_03_05a

2.602.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NO	Sicherheitsmodul befindet sich im Zustand "terminiert"

T_SUPPORTED-1	
CN- NO_CURRENT_EF- 2	Das EF ist ausgewählt
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN- WRONG_FILE_TYP E-2	Ausgewähltes EF ist transparent
CN- OFFSET_TOO_BIG- 2	Parameter "Offset" in Kommando-APDU ist nicht zu groß
CN- DATA_TOO_BIG-2	Parameter "neue Daten" ragt nicht über das Dateiende hinaus

2.602.4 APDU-Kommandos

ID: CM-UPDATE_BINARY_WITHOUT_SF1_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.602.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.602.6 Verifikationen

ID	Beschreibung

VF-UPDATE_BINARY_WITHOUT_SFI-2	Der ausgelesene Inhalt des entsprechenden EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

2.603 Testfall: UPDATE BINARY ohne SFI (TC_UPDATE_BINARY_WITHOUT_SFI_FF_2)

2.603.1 Informationen

ID	TC_UPDATE_BINARY_WITHOUT_SFI_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE BINARY ohne SFI nicht erfolgreich durchgeführt werden kann, wenn kein EF selektiert ist. Dazu wird eine Kommandonachricht für UPDATE BINARY ohne SFI zum Schreiben oder Aktualisieren eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.603.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_14a, VI_03_01a, VI_03_05a

2.603.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-CURRENT_EF-1	Das EF ist nicht ausgewählt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN- WRONG_FILE_TYP E-2	Ausgewähltes EF ist transparent
CN- OFFSET_TOO_BIG- 2	Parameter "Offset" in Kommando-APDU ist nicht zu groß
CN- DATA_TOO_BIG-2	Parameter "neue Daten" ragt nicht über das Dateende hinaus

2.603.4 APDU-Kommandos

ID: CM-UPDATE_BINARY_WITHOUT_SFI_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.603.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6986	Das Testsystem antwortet mit '69 86'.

2.603.6 Verifikationen

ID	Beschreibung
VF-UPDATE_BINARY_WITHOUT_SFI-2	Der ausgelesene Inhalt des entsprechenden EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

2.604 Testfall: UPDATE BINARY ohne SFI (TC_UPDATE_BINARY_WITHOUT_SFI_FF_3)

2.604.1 Informationen

ID	TC_UPDATE_BINARY_WITHOUT_SFI_FF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE BINARY ohne SFI nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Dazu wird eine Kommandonachricht für UPDATE BINARY ohne SFI zum Schreiben oder Aktualisieren eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.604.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_14a, VI_03_01a, VI_03_05a

2.604.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_CURRENT_EF-	Das EF ist ausgewählt

2	
CN-WRONG_FILE_TYP E-2	Ausgewähltes EF ist transparent
CN-OFFSET_TOO_BIG- 2	Parameter "Offset" in Kommando-APDU ist nicht zu groß
CN-DATA_TOO_BIG-2	Parameter "neue Daten" ragt nicht über das Dateiende hinaus

2.604.4 APDU-Kommandos

ID: CM-UPDATE_BINARY_WITHOUT_SFI_FF_3						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.604.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.604.6 Verifikationen

ID	Beschreibung
VF-UPDATE_BINARY_WITHOUT_SFI-2	Der ausgelesene Inhalt des entsprechenden EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

2.605 Testfall: UPDATE BINARY ohne SFI (TC_UPDATE_BINARY_WITHOUT_SFI_FF_4)

2.605.1 Informationen

ID	TC_UPDATE_BINARY_WITHOUT_SFI_FF_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE BINARY ohne SFI nicht erfolgreich durchgeführt werden kann, wenn das ausgewählte EF nicht transparent ist. Dazu wird eine Kommandonachricht für UPDATE BINARY ohne SFI zum Schreiben oder Aktualisieren eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.605.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_14a, VI_03_01a, VI_03_05a

2.605.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-WRONG_FILE_TYPE-1	Ausgewähltes EF ist nicht transparent
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_CURRENT_EF-2	Das EF ist ausgewählt

CN-SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN-OFFSET_TOO_BIG- 2	Parameter "Offset" in Kommando-APDU ist nicht zu groß
CN-DATA_TOO_BIG-2	Parameter "neue Daten" ragt nicht über das Dateiende hinaus

2.605.4 APDU-Kommandos

ID: CM-UPDATE_BINARY_WITHOUT_SFI_FF_4						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.605.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6981	Das Testsystem antwortet mit '69 81'.

2.605.6 Verifikationen

ID	Beschreibung
VF-UPDATE_BINARY_WITHOUT_SFI-2	Der ausgelesene Inhalt des entsprechenden EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

2.606 Testfall: UPDATE BINARY ohne SFI (TC_UPDATE_BINARY_WITHOUT_SFI_FF_5)

2.606.1 Informationen

ID	TC_UPDATE_BINARY_WITHOUT_SFI_FF_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE BINARY ohne SFI nicht erfolgreich durchgeführt werden kann, wenn der Parameter "Offset" in Kommando-APDU zu groß ist. Dazu wird eine Kommandonachricht für UPDATE BINARY ohne SFI zum Schreiben oder Aktualisieren eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.606.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_14a, VI_03_01a, VI_03_05a

2.606.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OFFSET_TOO_BIG-1	Parameter "Offset" in Kommando-APDU ist zu groß
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_CURRENT_EF-2	Das EF ist ausgewählt

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN- WRONG_FILE_TYP E-2	Ausgewähltes EF ist transparent
CN- DATA_TOO_BIG-2	Parameter "neue Daten" ragt nicht über das Dateiende hinaus

2.606.4 APDU-Kommandos

ID: CM-UPDATE_BINARY_WITHOUT_SFI_FF_5						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.606.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6B00	Das Testsystem antwortet mit '6b 00'.

2.606.6 Verifikationen

ID	Beschreibung
VF-UPDATE_BINARY_WITHOUT_SFI-2	Der ausgelesene Inhalt des entsprechenden EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

2.607 Testfall: UPDATE BINARY ohne SFI (TC_UPDATE_BINARY_WITHOUT_SFI_FF_6)

2.607.1 Informationen

ID	TC_UPDATE_BINARY_WITHOUT_SFI_FF_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE BINARY ohne SFI nicht erfolgreich durchgeführt werden kann, wenn der Parameter "neue Daten" über das Dateende hinausragt. Dazu wird eine Kommandonachricht für UPDATE BINARY ohne SFI zum Schreiben oder Aktualisieren eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.607.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.2

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_14a, VI_03_01a, VI_03_05a

2.607.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-DATA_TOO_BIG-1	Parameter "neue Daten" ragt über das Dateende hinaus
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_CURRENT_EF-2	Das EF ist ausgewählt

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN- WRONG_FILE_TYP E-2	Ausgewähltes EF ist transparent
CN- OFFSET_TOO_BIG- 2	Parameter "Offset" in Kommando-APDU ist nicht zu groß

2.607.4 APDU-Kommandos

ID: CM-UPDATE_BINARY_WITHOUT_SFI_FF_6						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält $(\text{Offset} - \text{P2}) / 256$, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.607.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A87	Das Testsystem antwortet mit '6a 87'.

2.607.6 Verifikationen

ID	Beschreibung
VF-UPDATE_BINARY_WITHOUT_SFI-2	Der ausgelesene Inhalt des entsprechenden EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

2.608 Testfall: UPDATE BINARY mit SFI (TC_UPDATE_BINARY_WITH_SFI_GF_1)

2.608.1 Informationen

ID	TC_UPDATE_BINARY_WITH_SFI_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE BINARY mit SFI erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für UPDATE BINARY mit SFI zum Schreiben oder Aktualisieren eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.608.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_14b, VI_03_01b, VI_03_05b

2.608.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt

CN-WRONG_FILE_TYP E-2	Ausgewähltes EF ist transparent
CN-OFFSET_TOO_BIG- 2	Parameter "Offset" in Kommando-APDU ist nicht zu groß
CN-DATA_TOO_BIG-2	Parameter "neue Daten" ragt nicht über das Dateende hinaus

2.608.4 APDU-Kommandos

ID: CM-UPDATE_BINARY_WITH_SFI_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält '80' + SFI.

'P2' enthält den Offset aus {'00', ..., 'FF'}.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.608.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.608.6 Verifikationen

ID	Beschreibung
VF-UPDATE_BINARY_WITH_SFI-1	Der ausgelesene Inhalt des entsprechenden EF stimmt mit dem entsprechenden Inhalt dieses Testfalls überein

2.609 Testfall: UPDATE BINARY mit SFI (TC_UPDATE_BINARY_WITH_SFI_FF_1)

2.609.1 Informationen

ID	TC_UPDATE_BINARY_WITH_SFI_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE BINARY mit SFI nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für UPDATE BINARY mit SFI zum Schreiben oder Aktualisieren eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.609.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_14b, VI_03_01b, VI_03_05b

2.609.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- INSTRUCTION_NO T_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN- FILE_NOT_FOUND- 2	Das per SFI adressierte File kann gefunden werden
CN- SECURITY_STATU S_NOT_SATISFIED-	Zugriffsregel ist erfüllt

2	
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist transparent
CN-OFFSET_TOO_BIG-2	Parameter "Offset" in Kommando-APDU ist nicht zu groß
CN-DATA_TOO_BIG-2	Parameter "neue Daten" ragt nicht über das Dateende hinaus

2.609.4 APDU-Kommandos

ID: CM-UPDATE_BINARY_WITH_SFI_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält '80' + SFI.

'P2' enthält den Offset aus {'00', ..., 'FF'}.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.609.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.609.6 Verifikationen

ID	Beschreibung
VF-UPDATE_BINARY_WITH_SFI-2	Der ausgelesene Inhalt des entsprechenden EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

2.610 Testfall: UPDATE BINARY mit SFI (TC_UPDATE_BINARY_WITH_SFI_FF_2)

2.610.1 Informationen

ID	TC_UPDATE_BINARY_WITH_SFI_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE BINARY mit SFI nicht erfolgreich durchgeführt werden kann, wenn das per SFI adressierte File nicht gefunden werden kann. Dazu wird eine Kommandonachricht für UPDATE BINARY mit SFI zum Schreiben oder Aktualisieren eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.610.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_14b, VI_03_01b, VI_03_05b

2.610.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- FILE_NOT_FOUND- 1	Das per SFI adressierte File kann nicht gefunden werden
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt

CN-WRONG_FILE_TYP E-2	Ausgewähltes EF ist transparent
CN-OFFSET_TOO_BIG- 2	Parameter "Offset" in Kommando-APDU ist nicht zu groß
CN-DATA_TOO_BIG-2	Parameter "neue Daten" ragt nicht über das Dateende hinaus

2.610.4 APDU-Kommandos

ID: CM-UPDATE_BINARY_WITH_SFI_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält '80' + SFI.

'P2' enthält den Offset aus {'00', ..., 'FF'}.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.610.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A82	Das Testsystem antwortet mit '6a 82'.

2.610.6 Verifikationen

ID	Beschreibung
VF-UPDATE_BINARY_WITH_SFI-2	Der ausgelesene Inhalt des entsprechenden EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

2.611 Testfall: UPDATE BINARY mit SFI (TC_UPDATE_BINARY_WITH_SFI_FF_3)

2.611.1 Informationen

ID	TC_UPDATE_BINARY_WITH_SFI_FF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE BINARY mit SFI nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Dazu wird eine Kommandonachricht für UPDATE BINARY mit SFI zum Schreiben oder Aktualisieren eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.611.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_14b, VI_03_01b, VI_03_05b

2.611.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN- SEMANTIC_CORRE CTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN- SECURITY_STATU S_NOT_SATISFIED- 1	Zugriffsregel ist nicht erfüllt
CN- INSTRUCTION_NO T_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN- FILE_NOT_FOUND-	Das per SFI adressierte File kann gefunden werden

2	
CN-WRONG_FILE_TYP E-2	Ausgewähltes EF ist transparent
CN-OFFSET_TOO_BIG- 2	Parameter "Offset" in Kommando-APDU ist nicht zu groß
CN-DATA_TOO_BIG-2	Parameter "neue Daten" ragt nicht über das Dateende hinaus

2.611.4 APDU-Kommandos

ID: CM-UPDATE_BINARY_WITH_SFI_FF_3						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält '80' + SFI.

'P2' enthält den Offset aus {'00', ..., 'FF'}.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.611.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.611.6 Verifikationen

ID	Beschreibung
VF-UPDATE_BINARY_WITH_SFI-2	Der ausgelesene Inhalt des entsprechenden EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

2.612 Testfall: UPDATE BINARY mit SFI (TC_UPDATE_BINARY_WITH_SFI_FF_4)

2.612.1 Informationen

ID	TC_UPDATE_BINARY_WITH_SFI_FF_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE BINARY mit SFI nicht erfolgreich durchgeführt werden kann, wenn das ausgewählte EF nicht transparent ist. Dazu wird eine Kommandonachricht für UPDATE BINARY mit SFI zum Schreiben oder Aktualisieren eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.612.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_14b, VI_03_01b, VI_03_05b

2.612.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-WRONG_FILE_TYPE-1	Ausgewähltes EF ist nicht transparent
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN- OFFSET_TOO_BIG- 2	Parameter "Offset" in Kommando-APDU ist nicht zu groß
CN- DATA_TOO_BIG-2	Parameter "neue Daten" ragt nicht über das Dateende hinaus

2.612.4 APDU-Kommandos

ID: CM-UPDATE_BINARY_WITH_SFI_FF_4						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält '80' + SFI.

'P2' enthält den Offset aus {'00', ..., 'FF'}.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.612.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6981	Das Testsystem antwortet mit '69 81'.

2.612.6 Verifikationen

ID	Beschreibung
VF-UPDATE_BINARY_WITH_SFI-2	Der ausgelesene Inhalt des entsprechenden EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

2.613 Testfall: UPDATE BINARY mit SFI (TC_UPDATE_BINARY_WITH_SFI_FF_5)

2.613.1 Informationen

ID	TC_UPDATE_BINARY_WITH_SFI_FF_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE BINARY mit SFI nicht erfolgreich durchgeführt werden kann, wenn der Parameter "Offset" in Kommando-APDU zu groß ist. Dazu wird eine Kommandonachricht für UPDATE BINARY mit SFI zum Schreiben oder Aktualisieren eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.613.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_14b, VI_03_01b, VI_03_05b

2.613.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OFFSET_TOO_BIG-1	Parameter "Offset" in Kommando-APDU ist zu groß
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN- WRONG_FILE_TYP E-2	Ausgewähltes EF ist transparent
CN- DATA_TOO_BIG-2	Parameter "neue Daten" ragt nicht über das Dateiende hinaus

2.613.4 APDU-Kommandos

ID: CM-UPDATE_BINARY_WITH_SFI_FF_5						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält '80' + SFI.

'P2' enthält den Offset aus {'00', ..., 'FF'}.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.613.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6B00	Das Testsystem antwortet mit '6b 00'.

2.613.6 Verifikationen

ID	Beschreibung
VF-UPDATE_BINARY_WITH_SFI-2	Der ausgelesene Inhalt des entsprechenden EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

2.614 Testfall: UPDATE BINARY mit SFI (TC_UPDATE_BINARY_WITH_SFI_FF_6)

2.614.1 Informationen

ID	TC_UPDATE_BINARY_WITH_SFI_FF_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE BINARY mit SFI nicht erfolgreich durchgeführt werden kann, wenn der Parameter "neue Daten" über das Dateiende hinausragt. Dazu wird eine Kommandonachricht für UPDATE BINARY mit SFI zum Schreiben oder Aktualisieren eines transparenten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.614.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.1

Der Testfall wird in folgenden Use-Cases referenziert: PN_04_14b, VI_03_01b, VI_03_05b

2.614.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-DATA_TOO_BIG-1	Parameter "neue Daten" ragt über das Dateiende hinaus
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN- WRONG_FILE_TYP E-2	Ausgewähltes EF ist transparent
CN- OFFSET_TOO_BIG- 2	Parameter "Offset" in Kommando-APDU ist nicht zu groß

2.614.4 APDU-Kommandos

ID: CM-UPDATE_BINARY_WITH_SFI_FF_6						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält '80' + SFI.

'P2' enthält den Offset aus {'00', ..., 'FF'}.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.614.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A87	Das Testsystem antwortet mit '6a 87'.

2.614.6 Verifikationen

ID	Beschreibung
VF-UPDATE_BINARY_WITH_SFI-2	Der ausgelesene Inhalt des entsprechenden EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

2.615 Testfall: UPDATE RECORD ohne SFI (TC_UPDATE_RECORD_WITHOUT_SFI_GF_1)

2.615.1 Informationen

ID	TC_UPDATE_RECORD_WITHOUT_SFI_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE RECORD ohne SFI erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für UPDATE RECORD ohne SFI zum Schreiben oder Aktualisieren eines record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.615.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.4

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_03a, PN_03_05a, VI_02_14a, VI_04_02a

2.615.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-CURRENT_EF-2	Das EF ist ausgewählt
CN-SECURITY_STATUSES_NOT_SATISFIED-	Zugriffsregel ist erfüllt

2	
CN-WRONG_FILE_TYP E-2	Ausgewähltes EF ist strukturiert
CN-RECORD_NOT_FO UND-2	Record-Nummer existiert
CN-WRONG_RECORD_ LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge
CN-OUT_OF_MEMORY -2	Speicherplatz des EF reicht aus

2.615.4 APDU-Kommandos

ID: CM-UPDATE_RECORD_WITHOUT_SFI_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.615.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

2.615.6 Verifikationen

ID	Beschreibung
VF-UPDATE_RECORD_WITHOUT_SFI-1	Der ausgelesene Inhalt des entsprechenden record-orientierten EF stimmt mit dem entsprechenden Inhalt dieses Testfalls überein

2.616 Testfall: UPDATE RECORD ohne SFI (TC_UPDATE_RECORD_WITHOUT_SFI_FF_1)

2.616.1 Informationen

ID	TC_UPDATE_RECORD_WITHOUT_SFI_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE RECORD ohne SFI nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für UPDATE RECORD ohne SFI zum Schreiben oder Aktualisieren eines record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.616.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.4

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_03a, PN_03_05a, VI_02_14a, VI_04_02a

2.616.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-CURRENT_EF-2	Das EF ist ausgewählt
CN-SECURITY_STATUS	Zugriffsregel ist erfüllt

S_NOT_SATISFIED-2	
CN-WRONG_FILE_TYP E-2	Ausgewähltes EF ist strukturiert
CN-RECORD_NOT_FO UND-2	Record-Nummer existiert
CN-WRONG_RECORD_LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge
CN-OUT_OF_MEMORY-2	Speicherplatz des EF reicht aus

2.616.4 APDU-Kommandos

ID: CM-UPDATE_RECORD_WITHOUT_SFI_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Nummer.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.616.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.616.6 Verifikationen

ID	Beschreibung
VF-UPDATE_RECORD_WITHOUT_SFI-2	Der ausgelesene Inhalt des entsprechenden record-orientierten EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht

	überein

2.617 Testfall: UPDATE RECORD ohne SFI (TC_UPDATE_RECORD_WITHOUT_SFI_FF_2)

2.617.1 Informationen

ID	TC_UPDATE_RECORD_WITHOUT_SFI_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE RECORD ohne SFI nicht erfolgreich durchgeführt werden kann, wenn kein EF selektiert ist. Dazu wird eine Kommandonachricht für UPDATE RECORD ohne SFI zum Schreiben oder Aktualisieren eines record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.617.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.4

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_03a, PN_03_05a, VI_02_14a, VI_04_02a

2.617.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-NO_CURRENT_EF-1	Das EF ist nicht ausgewählt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN- WRONG_FILE_TYP E-2	Ausgewähltes EF ist strukturiert
CN- RECORD_NOT_FO UND-2	Record-Nummer existiert
CN- WRONG_RECORD_ LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge
CN- OUT_OF_MEMORY -2	Speicherplatz des EF reicht aus

2.617.4 APDU-Kommandos

ID: CM-UPDATE_RECORD_WITHOUT_SFI_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.617.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6986	Das Testsystem antwortet mit '69 86'.

2.617.6 Verifikationen

ID	Beschreibung
VF-UPDATE_RECORD_WITHOUT_SFI-2	Der ausgelesene Inhalt des entsprechenden

	record-orientierten EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

2.618 Testfall: UPDATE RECORD ohne SFI (TC_UPDATE_RECORD_WITHOUT_SFI_FF_3)

2.618.1 Informationen

ID	TC_UPDATE_RECORD_WITHOUT_SFI_FF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE RECORD ohne SFI nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Dazu wird eine Kommandonachricht für UPDATE RECORD ohne SFI zum Schreiben oder Aktualisieren eines record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.618.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.4

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_03a, PN_03_05a, VI_02_14a, VI_04_02a

2.618.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt

CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_CURRENT_EF-2	Das EF ist ausgewählt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist strukturiert
CN-RECORD_NOT_FOUND-2	Record-Nummer existiert
CN-WRONG_RECORD_LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge
CN-OUT_OF_MEMORY-2	Speicherplatz des EF reicht aus

2.618.4 APDU-Kommandos

ID: CM-UPDATE_RECORD_WITHOUT_SFI_FF_3						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Nummer.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.618.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.618.6 Verifikationen

ID	Beschreibung
VF-UPDATE_RECORD_WITHOUT_SFI-2	Der ausgelesene Inhalt des entsprechenden record-orientierten EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

2.619 Testfall: UPDATE RECORD ohne SFI (TC_UPDATE_RECORD_WITHOUT_SFI_FF_4)

2.619.1 Informationen

ID	TC_UPDATE_RECORD_WITHOUT_SFI_FF_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE RECORD ohne SFI nicht erfolgreich durchgeführt werden kann, wenn das ausgewählte EF keine Record-basierte Struktur aufweist. Dazu wird eine Kommandonachricht für UPDATE RECORD ohne SFI zum Schreiben oder Aktualisieren eines record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.619.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.4

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_03a, PN_03_05a, VI_02_14a, VI_04_02a

2.619.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN-WRONG_FILE_TYPE-1	Ausgewähltes EF ist nicht strukturiert
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_CURRENT_EF-2	Das EF ist ausgewählt
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-RECORD_NOT_FOUND-2	Record-Nummer existiert
CN-WRONG_RECORD_LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge
CN-OUT_OF_MEMORY-2	Speicherplatz des EF reicht aus

2.619.4 APDU-Kommandos

ID: CM-UPDATE_RECORD_WITHOUT_SF_FF_4						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.619.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6981	Das Testsystem antwortet mit '69 81'.

2.619.6 Verifikationen

ID	Beschreibung
VF-UPDATE_RECORD_WITHOUT_SFI-2	Der ausgelesene Inhalt des entsprechenden record-orientierten EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

2.620 Testfall: UPDATE RECORD ohne SFI (TC_UPDATE_RECORD_WITHOUT_SFI_FF_5)

2.620.1 Informationen

ID	TC_UPDATE_RECORD_WITHOUT_SFI_FF_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE RECORD ohne SFI nicht erfolgreich durchgeführt werden kann, wenn die Record-Nummer nicht existiert. Dazu wird eine Kommandonachricht für UPDATE RECORD ohne SFI zum Schreiben oder Aktualisieren eines record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.620.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.4

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_03a, PN_03_05a, VI_02_14a, VI_04_02a

2.620.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-	Record-Nummer existiert nicht

RECORD_NOT_FOUND-1	
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_CURRENT_EF-2	Das EF ist ausgewählt
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist strukturiert
CN-WRONG_RECORD_LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge
CN-OUT_OF_MEMORY-2	Speicherplatz des EF reicht aus

2.620.4 APDU-Kommandos

ID: CM-UPDATE_RECORD_WITHOUT_SFI_FF_5						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.620.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A83	Das Testsystem antwortet mit '6a 83'.

2.620.6 Verifikationen

ID	Beschreibung
VF-UPDATE_RECORD_WITHOUT_SFI-2	Der ausgelesene Inhalt des entsprechenden record-orientierten EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

2.621 Testfall: UPDATE RECORD ohne SFI (TC_UPDATE_RECORD_WITHOUT_SFI_FF_6)

2.621.1 Informationen

ID	TC_UPDATE_RECORD_WITHOUT_SFI_FF_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE RECORD ohne SFI nicht erfolgreich durchgeführt werden kann, wenn die Länge der an das File anzuhängenden Daten nicht zulässig ist. Dazu wird eine Kommandonachricht für UPDATE RECORD ohne SFI zum Schreiben oder Aktualisieren eines record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.621.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.4

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_03a, PN_03_05a, VI_02_14a, VI_04_02a

2.621.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.

CN-WRONG_RECORD_LENGTH-1	Parameter "neue Daten" passt nicht zur zulässigen Record-Länge
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_CURRENT_EF-2	Das EF ist ausgewählt
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist strukturiert
CN-RECORD_NOT_FOUND-2	Record-Nummer existiert
CN-OUT_OF_MEMORY-2	Speicherplatz des EF reicht aus

2.621.4 APDU-Kommandos

ID: CM-UPDATE_RECORD_WITHOUT_SFI_FF_6						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.621.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A87	Das Testsystem antwortet mit '6a 87'.

2.621.6 Verifikationen

ID	Beschreibung
VF-UPDATE_RECORD_WITHOUT_SFI-2	Der ausgelesene Inhalt des entsprechenden record-orientierten EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

2.622 Testfall: UPDATE RECORD ohne SFI (TC_UPDATE_RECORD_WITHOUT_SFI_FF_7)

2.622.1 Informationen

ID	TC_UPDATE_RECORD_WITHOUT_SFI_FF_7
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE RECORD ohne SFI nicht erfolgreich durchgeführt werden kann, wenn der restliche Speicherplatz des EF nicht ausreicht. Dazu wird eine Kommandonachricht für UPDATE RECORD ohne SFI zum Schreiben oder Aktualisieren eines record-orientierten EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.622.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.4

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_03a, PN_03_05a, VI_02_14a, VI_04_02a

2.622.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-	Speicherplatz des EF reicht nicht aus

OUT_OF_MEMORY-1	
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-NO_CURRENT_EF-2	Das EF ist ausgewählt
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist strukturiert
CN-RECORD_NOT_FOUND-2	Record-Nummer existiert
CN-WRONG_RECORD_LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge

2.622.4 APDU-Kommandos

ID: CM-UPDATE_RECORD_WITHOUT_SFI_FF_7						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Nummer.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.622.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A84	Das Testsystem antwortet mit '6a 84'.

2.622.6 Verifikationen

ID	Beschreibung
VF-UPDATE_RECORD_WITHOUT_SFI-2	Der ausgelesene Inhalt des entsprechenden record-orientierten EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

2.623 Testfall: UPDATE RECORD mit SFI (TC_UPDATE_RECORD_WITH_SFI_GF_1)

2.623.1 Informationen

ID	TC_UPDATE_RECORD_WITH_SFI_GF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE RECORD mit SFI erfolgreich durchgeführt werden kann, sofern alle notwendigen Voraussetzungen erfüllt sind. Dazu wird eine Kommandonachricht für UPDATE RECORD mit SFI zum Schreiben oder Aktualisieren eines record-orientierte EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Gutfall-Test

2.623.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.4

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_03b, PN_03_05b, VI_02_14b, VI_04_02b

2.623.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

INSTRUCTION_NO T_SUPPORTED-2	
CN- FILE_NOT_FOUND- 2	Das per SFI adressierte File kann gefunden werden
CN- SECURITY_STATU S_NOT_SATISFIED- 2	Zugriffsregel ist erfüllt
CN- WRONG_FILE_TYP E-2	Ausgewähltes EF ist strukturiert
CN- RECORD_NOT_FO UND-2	Record-Nummer existiert
CN- WRONG_RECORD_ LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge
CN- OUT_OF_MEMORY -2	Speicherplatz des EF reicht aus

2.623.4 APDU-Kommandos

ID: CM-UPDATE_RECORD_WITH_SFI_GF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	XX	LL	XX...XX	--

'P1' enthält die Record-Number.

'P2' enthält (SFI << 3) + '04' (Update Record der Nummer wie in P1 angegeben)

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.623.5 Erwartete Ergebnisse

ID	Beschreibung

RS-9000	Das Testsystem antwortet mit '90 00'.

2.623.6 Verifikationen

ID	Beschreibung
VF-UPDATE_RECORD_WITH_SFI-1	Der ausgelesene Inhalt des entsprechenden record-orientierten EF stimmt mit dem entsprechenden Inhalt dieses Testfalls überein

2.624 Testfall: UPDATE RECORD mit SFI (TC_UPDATE_RECORD_WITH_SFI_FF_1)

2.624.1 Informationen

ID	TC_UPDATE_RECORD_WITH_SFI_FF_1
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE RECORD mit SFI nicht erfolgreich durchgeführt werden kann, wenn sich das Sicherheitsmodul im Zustand "terminiert" befindet. Dazu wird eine Kommandonachricht für UPDATE RECORD mit SFI zum Schreiben oder Aktualisieren eines record-orientierte EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.624.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.4

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_03b, PN_03_05b, VI_02_14b, VI_04_02b

2.624.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft

SEMANTIC_CORRECTNESS	(soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-INSTRUCTION_NOT_SUPPORTED-1	Sicherheitsmodul befindet sich im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist strukturiert
CN-RECORD_NOT_FOUND-2	Record-Nummer existiert
CN-WRONG_RECORD_LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge
CN-OUT_OF_MEMORY-2	Speicherplatz des EF reicht aus

2.624.4 APDU-Kommandos

ID: CM-UPDATE_RECORD_WITH_SFI_FF_1						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	XX	LL	XX...XX	--

'P1' enthält die Record-Number.

'P2' enthält (SFI << 3) + '04' (Update Record der Nummer wie in P1 angegeben)

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.624.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6D00	Das Testsystem antwortet mit '6d 00'.

2.624.6 Verifikationen

ID	Beschreibung
VF-UPDATE_RECORD_WITH_SFI-2	Der ausgelesene Inhalt des entsprechenden record-orientierten EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

2.625 Testfall: UPDATE RECORD mit SFI (TC_UPDATE_RECORD_WITH_SFI_FF_2)

2.625.1 Informationen

ID	TC_UPDATE_RECORD_WITH_SFI_FF_2
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE RECORD mit SFI nicht erfolgreich durchgeführt werden kann, wenn das per SFI adressierte File nicht gefunden werden kann. Dazu wird eine Kommandonachricht für UPDATE RECORD mit SFI zum Schreiben oder Aktualisieren eines record-orientierte EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.625.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.4

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_03b, PN_03_05b, VI_02_14b, VI_04_02b

2.625.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-FILE_NOT_FOUND-1	Das per SFI adressierte File kann nicht gefunden werden
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist strukturiert
CN-RECORD_NOT_FOUND-2	Record-Nummer existiert
CN-WRONG_RECORD_LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge
CN-OUT_OF_MEMORY-2	Speicherplatz des EF reicht aus

2.625.4 APDU-Kommandos

ID: CM-UPDATE_RECORD_WITH_SFI_FF_2						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	XX	LL	XX...XX	--

'P1' enthält die Record-Nummer.

'P2' enthält (SFI << 3) + '04' (Update Record der Nummer wie in P1 angegeben)

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.625.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A82	Das Testsystem antwortet mit '6a 82'.

2.625.6 Verifikationen

ID	Beschreibung
VF-UPDATE_RECORD_WITH_SFI-2	Der ausgelesene Inhalt des entsprechenden record-orientierten EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

2.626 Testfall: UPDATE RECORD mit SFI (TC_UPDATE_RECORD_WITH_SFI_FF_3)

2.626.1 Informationen

ID	TC_UPDATE_RECORD_WITH_SFI_FF_3
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE RECORD mit SFI nicht erfolgreich durchgeführt werden kann, wenn die Zugriffsregeln im Kontext des Objekts nicht erfüllt sind. Dazu wird eine Kommandonachricht für UPDATE RECORD mit SFI zum Schreiben oder Aktualisieren eines record-orientierte EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.626.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.4

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_03b, PN_03_05b, VI_02_14b, VI_04_02b

2.626.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-SECURITY_STATUSES_NOT_SATISFIED-1	Zugriffsregel ist nicht erfüllt
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist strukturiert
CN-RECORD_NOT_FOUND-2	Record-Nummer existiert
CN-WRONG_RECORD_LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge
CN-OUT_OF_MEMORY-2	Speicherplatz des EF reicht aus

2.626.4 APDU-Kommandos

ID: CM-UPDATE_RECORD_WITH_SFI_FF_3						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	XX	LL	XX...XX	--

'P1' enthält die Record-Number.

'P2' enthält (SFI << 3) + '04' (Update Record der Nummer wie in P1 angegeben)

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.626.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

2.626.6 Verifikationen

ID	Beschreibung
VF-UPDATE_RECORD_WITH_SFI-2	Der ausgelesene Inhalt des entsprechenden record-orientierten EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

2.627 Testfall: UPDATE RECORD mit SFI (TC_UPDATE_RECORD_WITH_SFI_FF_4)

2.627.1 Informationen

ID	TC_UPDATE_RECORD_WITH_SFI_FF_4
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE RECORD mit SFI nicht erfolgreich durchgeführt werden kann, wenn das ausgewählte EF keine Record-basierte Struktur aufweist. Dazu wird eine Kommandonachricht für UPDATE RECORD mit SFI zum Schreiben oder Aktualisieren eines record-orientierte EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.627.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.4

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_03b, PN_03_05b, VI_02_14b, VI_04_02b

2.627.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-WRONG_FILE_TYPE-1	Ausgewähltes EF ist nicht strukturiert
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-RECORD_NOT_FOUND-2	Record-Nummer existiert
CN-WRONG_RECORD_LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge
CN-OUT_OF_MEMORY-2	Speicherplatz des EF reicht aus

2.627.4 APDU-Kommandos

ID: CM-UPDATE_RECORD_WITH_SFI_FF_4						
CLA	INS	P1	P2	Lc	Data	Le

00	dc	XX	XX	LL	XX...XX	--

'P1' enthält die Record-Number.

'P2' enthält (SFI << 3) + '04' (Update Record der Nummer wie in P1 angegeben)

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.627.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6981	Das Testsystem antwortet mit '69 81'.

2.627.6 Verifikationen

ID	Beschreibung
VF-UPDATE_RECORD_WITH_SFI-2	Der ausgelesene Inhalt des entsprechenden record-orientierten EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

2.628 Testfall: UPDATE RECORD mit SFI (TC_UPDATE_RECORD_WITH_SFI_FF_5)

2.628.1 Informationen

ID	TC_UPDATE_RECORD_WITH_SFI_FF_5
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE RECORD mit SFI nicht erfolgreich durchgeführt werden kann, wenn die Record-Nummer nicht existiert. Dazu wird eine Kommandonachricht für UPDATE RECORD mit SFI zum Schreiben oder Aktualisieren eines record-orientierte EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.628.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.4

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_03b, PN_03_05b, VI_02_14b, VI_04_02b

2.628.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-RECORD_NOT_FOUND-1	Record-Nummer existiert nicht
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist strukturiert
CN-WRONG_RECORD_LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge
CN-OUT_OF_MEMORY-2	Speicherplatz des EF reicht aus

2.628.4 APDU-Kommandos

ID: CM-UPDATE_RECORD_WITH_SFI_FF_5						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	XX	LL	XX...XX	--

'P1' enthält die Record-Number.

'P2' enthält (SFI << 3) + '04' (Update Record der Nummer wie in P1 angegeben)

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.628.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A83	Das Testsystem antwortet mit '6a 83'.

2.628.6 Verifikationen

ID	Beschreibung
VF-UPDATE_RECORD_WITH_SFI-2	Der ausgelesene Inhalt des entsprechenden record-orientierten EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

2.629 Testfall: UPDATE RECORD mit SFI (TC_UPDATE_RECORD_WITH_SFI_FF_6)

2.629.1 Informationen

ID	TC_UPDATE_RECORD_WITH_SFI_FF_6
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE RECORD mit SFI nicht erfolgreich durchgeführt werden kann, wenn die Länge der an das File anzuhängenden Daten nicht zulässig ist. Dazu wird eine Kommandonachricht für UPDATE RECORD mit SFI zum Schreiben oder Aktualisieren eines record-orientierte EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der

	Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.629.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.4

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_03b, PN_03_05b, VI_02_14b, VI_04_02b

2.629.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-WRONG_RECORD_LENGTH-1	Parameter "neue Daten" passt nicht zur zulässigen Record-Länge
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist strukturiert
CN-RECORD_NOT_FOUND-2	Record-Nummer existiert
CN-OUT_OF_MEMORY	Speicherplatz des EF reicht aus

-2	

2.629.4 APDU-Kommandos

ID: CM-UPDATE_RECORD_WITH_SFI_FF_6						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	XX	LL	XX...XX	--

'P1' enthält die Record-Number.

'P2' enthält (SFI << 3) + '04' (Update Record der Nummer wie in P1 angegeben)

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.629.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A87	Das Testsystem antwortet mit '6a 87'.

2.629.6 Verifikationen

ID	Beschreibung
VF-UPDATE_RECORD_WITH_SFI-2	Der ausgelesene Inhalt des entsprechenden record-orientierten EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

2.630 Testfall: UPDATE RECORD mit SFI (TC_UPDATE_RECORD_WITH_SFI_FF_7)

2.630.1 Informationen

ID	TC_UPDATE_RECORD_WITH_SFI_FF_7
Beschreibung	Dieser Test verifiziert, dass ein Kommando UPDATE RECORD mit SFI nicht erfolgreich durchgeführt werden kann, wenn der restliche Speicherplatz des EF nicht ausreicht. Dazu wird eine Kommandonachricht

	für UPDATE RECORD mit SFI zum Schreiben oder Aktualisieren eines record-orientierte EFs an das Sicherheitsmodul gesendet. Der Testfall prüft nur die erfolgreiche Ausführung des Kommandos. Die inhaltliche Korrektheit der Daten wird im Rahmen der Usecase-Tests überprüft.
Klassifizierung	Fehlerfall-Test

2.630.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 4.3.4

Der Testfall wird in folgenden Use-Cases referenziert: PN_02_03b, PN_03_05b, VI_02_14b, VI_04_02b

2.630.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-SEMANTIC_CORRECTNESS	Die im Testfall benutzten Daten sind semantisch korrekt. Dies betrifft (soweit in diesem Testfall vorhanden) Ein- und Ausgabedaten.
CN-OUT_OF_MEMORY-1	Speicherplatz des EF reicht nicht aus
CN-INSTRUCTION_NOT_SUPPORTED-2	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-FILE_NOT_FOUND-2	Das per SFI adressierte File kann gefunden werden
CN-SECURITY_STATUSES_NOT_SATISFIED-2	Zugriffsregel ist erfüllt
CN-WRONG_FILE_TYPE-2	Ausgewähltes EF ist strukturiert
CN-RECORD_NOT_FOUND	Record-Nummer existiert

UND-2	
CN-WRONG_RECORD_LENGTH-2	Parameter "neue Daten" passt zur zulässigen Record-Länge

2.630.4 APDU-Kommandos

ID: CM-UPDATE_RECORD_WITH_SFI_FF_7						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	XX	LL	XX...XX	--

'P1' enthält die Record-Number.

'P2' enthält (SFI << 3) + '04' (Update Record der Nummer wie in P1 angegeben)

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

2.630.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6A84	Das Testsystem antwortet mit '6a 84'.

2.630.6 Verifikationen

ID	Beschreibung
VF-UPDATE_RECORD_WITH_SFI-2	Der ausgelesene Inhalt des entsprechenden record-orientierten EF stimmt mit dem entsprechenden Inhalt dieses Testfalls nicht überein

3 Funktions-Tests

3.1 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_1)

3.1.1 Informationen

ID	TC_Funktion_IFO_1
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im MF des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des SELECT-Kommandos, ob das MF im initialen Dateisystem vorhanden ist. Die Durchführung erfolgt für MF.
Klassifizierung	Gutfall-Test

3.1.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.1.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1.4 APDU-Kommandos

ID: CM-Funktion_IFO_1						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	00	0c	02	3f00	--

3.1.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.2 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_2_1)

3.2.1 Informationen

ID	TC_Funktion_IFO_2_1
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im MF des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des SELECT-Kommandos, ob alle EFs im MF des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das technische Datenfeld für die Sicherheitsmodul-relevante Spezifikation EF.SecModTRInfo.
Klassifizierung	Gutfall-Test

3.2.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.2.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.2.4 APDU-Kommandos

ID: CM-Funktion_IFO_2_1						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	02	0c	02	01 1a	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

3.2.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.3 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_2_2)

3.3.1 Informationen

ID	TC_Funktion_IFO_2_2
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im MF des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des SELECT-Kommandos, ob alle EFs im MF des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das technische Datenfeld für die Sicherheitsmodul-relevante PACE-Funktionalität EF.SecModAccess.
Klassifizierung	Gutfall-Test

3.3.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.3.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.3.4 APDU-Kommandos

ID: CM-Funktion_IFO_2_2						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	02	0c	02	01 1b	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

3.3.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.4 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_2_3)

3.4.1 Informationen

ID	TC_Funktion_IFO_2_3
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im MF des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des SELECT-Kommandos, ob alle EFs im MF des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das technische Datenfeld für die Sicherheitsmodul-relevante PACE-Funktionalität EF.SecModCrypto.
Klassifizierung	Gutfall-Test

3.4.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.4.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.4.4 APDU-Kommandos

ID: CM-Funktion_IFO_2_3						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	02	0c	02	01 1c	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

3.4.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.5 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_2_4)

3.5.1 Informationen

ID	TC_Funktion_IFO_2_4
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im MF des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des SELECT-Kommandos, ob alle EFs im MF des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das technische Datenfeld für die Sicherheitsmodul-relevante PACE-Funktionalität EF.SecModLifeCycle.
Klassifizierung	Gutfall-Test

3.5.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.5.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.5.4 APDU-Kommandos

ID: CM-Funktion_IFO_2_4						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	02	0c	02	01 1d	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

3.5.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.6 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_3a_1)

3.6.1 Informationen

ID	TC_Funktion_IFO_3a_1
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im MF des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des MSE-Set-Kommandos, ob alle Key-Pair-Objekte für DST im MF des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Public Key-Objekt für GW-Admin-Schlüssel bzgl. TLS, also GWADM_TLS_PUB (Key.GWA_TLS_1).
Klassifizierung	Gutfall-Test

3.6.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.6.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.6.4 APDU-Kommandos

ID: CM-Funktion_IFO_3a_1						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	1c	80 0a [09 04 00 7f 00 07 01 01 04 01] 83 04 [00 00 00 11]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

3.6.5 Erwartete Ergebnisse

ID	Beschreibung

RS-7813	Das Key-Objekt 'Key.GWA_TLS_1' ist vorhanden.

3.7 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_3a_2)

3.7.1 Informationen

ID	TC_Funktion_IFO_3a_2
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im MF des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des MSE-Set-Kommandos, ob alle Key-Pair-Objekte für DST im MF des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Public Key-Objekt für GW-Admin-Schlüssel bzgl. SIG, also GWADM_SIG_PUB (Key.GWA_SIG_1).
Klassifizierung	Gutfall-Test

3.7.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.7.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.7.4 APDU-Kommandos

ID: CM-Funktion_IFO_3a_2						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	1c	80 0a [09 04 00 7f 00 07 01 01 04 01] 83 04 [00 00 00 12]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
|| '83-L83-Key Reference' (für das Public Key-Objekt)

3.7.5 Erwartete Ergebnisse

ID	Beschreibung
RS-45F2	Das Key-Objekt 'Key.GWA_SIG_1' ist vorhanden.

3.8 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_3a_3)

3.8.1 Informationen

ID	TC_Funktion_IFO_3a_3
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im MF des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des MSE-Set-Kommandos, ob alle Key-Pair-Objekte für DST im MF des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Public Key-Objekt für GW-Admin-Schlüssel bzgl. TLS, also GWADM_TLS_PUB (Key.GWA_TLS_2).
Klassifizierung	Gutfall-Test

3.8.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.8.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.8.4 APDU-Kommandos

ID: CM-Funktion_IFO_3a_3						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	1c	80 0a [09 04 00 7f 00 07 01 01 04 01] 83 04 [00 00 00 21]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

3.8.5 Erwartete Ergebnisse

ID	Beschreibung
RS-8C06	Das Key-Objekt 'Key.GWA_TLS_2' ist vorhanden.

3.9 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_3a_4)

3.9.1 Informationen

ID	TC_Funktion_IFO_3a_4
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im MF des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des MSE-Set-Kommandos, ob alle Key-Pair-Objekte für DST im MF des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Public Key-Objekt für GW-Admin-Schlüssel bzgl. SIG, also GWADM_SIG_PUB (Key.GWA_SIG_2).
Klassifizierung	Gutfall-Test

3.9.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.9.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.9.4 APDU-Kommandos

ID: CM-Funktion_IFO_3a_4						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	1c	80 0a [09 04 00 7f 00 07 01 01 04 01] 83 04	--

					[00 00 00 22]	

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

3.9.5 Erwartete Ergebnisse

ID	Beschreibung
RS-4574	Das Key-Objekt 'Key.GWA_SIG_2' ist vorhanden.

3.10 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_3a_5)

3.10.1 Informationen

ID	TC_Funktion_IFO_3a_5
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im MF des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des MSE-Set-Kommandos, ob alle Key-Pair-Objekte für DST im MF des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Public Key-Objekt für Transport-Import-Schlüssel, also IMP_PUB_TRANS (Key.IMP_PUB_TRANS).
Klassifizierung	Gutfall-Test

3.10.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.10.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.10.4 APDU-Kommandos

ID: CM-Funktion_IFO_3a_5

CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	1c	80 0a [09 04 00 7f 00 07 01 01 04 01] 83 04 [00 00 00 31]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

3.10.5 Erwartete Ergebnisse

ID	Beschreibung
RS-4CBF	Das Key-Objekt 'Key.IMP_PUB_TRANS' ist vorhanden.

3.11 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_3a_6)

3.11.1 Informationen

ID	TC_Funktion_IFO_3a_6
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im MF des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des MSE-Set-Kommandos, ob alle Key-Pair-Objekte für DST im MF des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Public Key-Objekt für Import-Schlüssel (Integrator-spezifisch), also IMP_PUB (Key.IMP_PUB).
Klassifizierung	Gutfall-Test

3.11.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.11.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.11.4 APDU-Kommandos

ID: CM-Funktion_IFO_3a_6						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	b6	1c	80 0a [09 04 00 7f 00 07 01 01 04 03] 83 04 [00 00 00 32]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
|| '83-L83-Key Reference' (für das Public Key-Objekt)

3.11.5 Erwartete Ergebnisse

ID	Beschreibung
RS-03F2	Das Key-Objekt 'Key.IMP_PUB' ist vorhanden.

3.12 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_3b_7)

3.12.1 Informationen

ID	TC_Funktion_IFO_3b_7
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im MF des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des MSE-Set-Kommandos, ob alle Key-Pair-Objekte für DST im MF des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Key-Pair-Objekt für Transport-Import-Schlüsselpaar, also (IMP_PRV_TRANS, IMP_PUB_TRANS). (Key.IMP_TRANS).
Klassifizierung	Gutfall-Test

3.12.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.12.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.12.4 APDU-Kommandos

ID: CM-Funktion_IFO_3b_7							
CLA	INS	P1	P2	Lc	Data	Le	
00	22	41	b6	0f	80 0a [09 04 00 7f 00 07 01 01 04 03] 83 01 [31]	--	

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '84-01-Key Reference' (für das Key Pair-Objekt)

3.12.5 Erwartete Ergebnisse

ID	Beschreibung
RS-C146	Das Key-Objekt 'Key.IMP_TRANS' ist vorhanden.

3.13 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_3b_8)

3.13.1 Informationen

ID	TC_Funktion_IFO_3b_8
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im MF des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des MSE-Set-Kommandos, ob alle Key-Pair-Objekte für DST im MF des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Key-Pair-Objekt für Import-Schlüsselpaar (Integrator-spezifisch), also (IMP_PRV, IMP_PUB) (Key.IMP).
Klassifizierung	Gutfall-Test

3.13.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.13.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.13.4 APDU-Kommandos

ID: CM-Funktion_IFO_3b_8						
CLA	INS	P1	P2	Lc	Data	Le
00	22	41	b6	0f	80 0a [09 04 00 7f 00 07 01 01 04 03] 83 01 [32]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '84-01-Key Reference' (für das Key Pair-Objekt)

3.13.5 Erwartete Ergebnisse

ID	Beschreibung
RS-1929	Das Key-Objekt 'Key.IMP' ist vorhanden.

3.14 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_3c_9)

3.14.1 Informationen

ID	TC_Funktion_IFO_3c_9
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im MF des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des MSE-Set-Kommandos, ob alle Key-Pair-Objekte für AT im MF des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Public Key-Objekt für GW-Admin-Schlüssel bzgl. ENC, also GWADM_ENC_PUB (Key.GWA_ENC_1).
Klassifizierung	Gutfall-Test

3.14.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.14.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.14.4 APDU-Kommandos

ID: CM-Funktion_IFO_3c_9						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	a4	12	80 0a [0A 04 00 7F 00 07 01 01 04 01 03] 83 04 [00 00 00 13]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

3.14.5 Erwartete Ergebnisse

ID	Beschreibung
RS-4DFF	Das Key-Objekt 'Key.GWA_ENC_1' ist vorhanden.

3.15 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_3c_10)

3.15.1 Informationen

ID	TC_Funktion_IFO_3c_10
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im MF des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des MSE-Set-Kommandos, ob alle Key-Pair-Objekte für AT im MF des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Public Key-Objekt für GW-Admin-Schlüssel bzgl. AUT, also GWADM_AUT_PUB (Key.GWA_AUT_1).

Klassifizierung	Gutfall-Test

3.15.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.15.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.15.4 APDU-Kommandos

ID: CM-Funktion_IFO_3c_10						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	a4	12	80 0a [0A 04 00 7F 00 07 01 01 04 01 03] 83 04 [00 00 00 10]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

3.15.5 Erwartete Ergebnisse

ID	Beschreibung
RS-566A	Das Key-Objekt 'Key.GWA_AUT_1' ist vorhanden.

3.16 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_3c_11)

3.16.1 Informationen

ID	TC_Funktion_IFO_3c_11
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im MF des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des MSE-Set-Kommandos, ob alle Key-Pair-Objekte für AT im MF des initialen

	Dateisystems vorhanden sind. Die Durchführung erfolgt für das Public Key-Objekt für GW-Admin-Schlüssel bzgl. ENC, also GWADM_ENC_PUB (Key.GWA_ENC_2).
Klassifizierung	Gutfall-Test

3.16.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.16.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.16.4 APDU-Kommandos

ID: CM-Funktion_IFO_3c_11						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	a4	12	80 0a [0A 04 00 7F 00 07 01 01 04 01 03] 83 04 [00 00 00 23]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

3.16.5 Erwartete Ergebnisse

ID	Beschreibung
RS-19CA	Das Key-Objekt 'Key.GWA_ENC_2' ist vorhanden.

3.17 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_3c_12)

3.17.1 Informationen

ID	TC_Funktion_IFO_3c_12

Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im MF des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des MSE-Set-Kommandos, ob alle Key-Pair-Objekte für AT im MF des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Public Key-Objekt für GW-Admin-Schlüssel bzgl. AUT, also GWADM_AUT_PUB (Key.GWA_AUT_2).
Klassifizierung	Gutfall-Test

3.17.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.17.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.17.4 APDU-Kommandos

ID: CM-Funktion_IFO_3c_12						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	a4	12	80 0a [0A 04 00 7F 00 07 01 01 04 01 03] 83 04 [00 00 00 20]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

3.17.5 Erwartete Ergebnisse

ID	Beschreibung
RS-4CE0	Das Key-Objekt 'Key.GWA_AUT_2' ist vorhanden.

3.18 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_4)

3.18.1 Informationen

ID	TC_Funktion_IFO_4
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im MF des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des CHANGE REFERENCE DATA Kommandos zum Setzen der PIN, ob das PIN-Objekt im MF des initialen Dateisystems vorhanden ist (PIN.GW).
Klassifizierung	Gutfall-Test

3.18.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.18.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.18.4 APDU-Kommandos

ID: CM-Funktion_IFO_4						
CLA	INS	P1	P2	Lc	Data	Le
00	24	01	01	06	31 32 33 34 35 36	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die neue PIN.

3.18.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.19 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_5)

3.19.1 Informationen

ID	TC_Funktion_IFO_5
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im DF.SMGW des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des SELECT-Kommandos, ob das DF.SMGW vorhanden ist.
Klassifizierung	Gutfall-Test

3.19.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.19.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.19.4 APDU-Kommandos

ID: CM-Funktion_IFO_5						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	00	0c	02	1001	--

'Data' enthält den File-Identifizier des zu selektierenden DF.

3.19.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.20 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_6_1)

3.20.1 Informationen

ID	TC_Funktion_IFO_6_1
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im DF.SMGW des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des SELECT-Kommandos, ob alle EFs im DF.SMGW des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für die Datenfelder für die SM-PKI-Root-Zertifikate (EF.SMPKIRoot_x).
Klassifizierung	Gutfall-Test

3.20.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.20.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.20.4 APDU-Kommandos

ID: CM-Funktion_IFO_6_1						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	01 XX	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

3.20.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.21 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_6_2)

3.21.1 Informationen

ID	TC_Funktion_IFO_6_2
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im DF.SMGW des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des SELECT-Kommandos, ob alle EFs im DF.SMGW des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Datenfeld für das Gütesiegel-Zertifikat bzgl. TLS (EF.GSCert_TLS).
Klassifizierung	Gutfall-Test

3.21.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.21.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.21.4 APDU-Kommandos

ID: CM-Funktion_IFO_6_2						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	01 11	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

3.21.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.22 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_6_3)

3.22.1 Informationen

ID	TC_Funktion_IFO_6_3
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im DF.SMGW des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des SELECT-Kommandos, ob alle EFs im DF.SMGW des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Datenfeld für das Gütesiegel-Zertifikat bzgl. SIG (EF.GSCert_SIG).
Klassifizierung	Gutfall-Test

3.22.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.22.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.22.4 APDU-Kommandos

ID: CM-Funktion_IFO_6_3						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	01 12	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

3.22.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.23 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_6_4)

3.23.1 Informationen

ID	TC_Funktion_IFO_6_4
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im DF.SMGW des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des SELECT-Kommandos, ob alle EFs im DF.SMGW des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Datenfeld für das Gütesiegel-Zertifikat bzgl. ENC (EF.GSCert_ENC).
Klassifizierung	Gutfall-Test

3.23.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.23.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.23.4 APDU-Kommandos

ID: CM-Funktion_IFO_6_4						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	01 13	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

3.23.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.24 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_6_5)

3.24.1 Informationen

ID	TC_Funktion_IFO_6_5
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im DF.SMGW des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des SELECT-Kommandos, ob alle EFs im DF.SMGW des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Datenfeld für die symmetrischen GW-Keys (EF.GWKeys).
Klassifizierung	Gutfall-Test

3.24.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.24.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.24.4 APDU-Kommandos

ID: CM-Funktion_IFO_6_5						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	01 14	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

3.24.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.25 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_7a_1)

3.25.1 Informationen

ID	TC_Funktion_IFO_7a_1
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im DF.SMGW des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des MSE-Set-Kommandos, ob alle Key-Pair-Objekte für DST im DF.SMGW des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Public-Key-Objekt für die SM-PKI-Root-Keys (Key.SMPKIRoot_x).
Klassifizierung	Gutfall-Test

3.25.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.25.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.25.4 APDU-Kommandos

ID: CM-Funktion_IFO_7a_1						
CLA	INS	P1	P2	Lc	Data	Le
00	22	41	b6	12	80 0a [09 04 00 7f 00 07 01 01 04 01] 83 04 [00 00 00 XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
|| '83-L83-Key Reference' (für das Public Key-Objekt)

3.25.5 Erwartete Ergebnisse

ID	Beschreibung
RS-1155	Das Key-Objekt 'Key.SMPKIRoot_x' ist vorhanden.

3.26 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_7a_2)

3.26.1 Informationen

ID	TC_Funktion_IFO_7a_2
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im DF.SMGW des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des MSE-Set-Kommandos, ob alle Key-Pair-Objekte für DST im DF.SMGW des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Public-Key-Objekte für CA-Public Key (relevant für die Prüfung von Zertifikatsketten im Rahmen der SM-PKI) (Key.CA_x).
Klassifizierung	Gutfall-Test

3.26.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.26.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.26.4 APDU-Kommandos

ID: CM-Funktion_IFO_7a_2						
CLA	INS	P1	P2	Lc	Data	Le
00	22	41	b6	12	80 0a [09 04 00 7f 00 07 01 01 04 01] 83 04 [00 00 01 XX]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
|| '83-L83-Key Reference' (für das Public Key-Objekt)

3.26.5 Erwartete Ergebnisse

ID	Beschreibung

RS-FD8B	Das Key-Objekt 'Key.CA_x' ist vorhanden.

3.27 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_7b_3)

3.27.1 Informationen

ID	TC_Funktion_IFO_7b_3
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im DF.SMGW des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des MSE-Set-Kommandos, ob alle Key-Pair-Objekte für DST im DF.SMGW des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Key Pair-Objekt für vorläufiges GW-Schlüsselpaar bzgl. TLS, also (GW_WAN_TLS_PRV_PRE, GW_WAN_TLS_PUB_PRE (Key.WAN_TLS_PRE)).
Klassifizierung	Gutfall-Test

3.27.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.27.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.27.4 APDU-Kommandos

ID: CM-Funktion_IFO_7b_3						
CLA	INS	P1	P2	Lc	Data	Le
00	22	41	b6	0f	80 0a [09 04 00 7f 00 07 01 01 04 01] 83 01 [01]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
|| '83-L83-Key Reference' (für das Public Key-Objekt)

3.27.5 Erwartete Ergebnisse

ID	Beschreibung
RS-03C3	Das Key-Objekt 'Key.WAN_TLS_PRE' ist vorhanden.

3.28 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_7b_4)

3.28.1 Informationen

ID	TC_Funktion_IFO_7b_4
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im DF.SMGW des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des MSE-Set-Kommandos, ob alle Key-Pair-Objekte für DST im DF.SMGW des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Key Pair-Objekt für vorläufiges GW-Schlüsselpaar bzgl. SIG, also (GW_WAN_SIG_PRV_PRE, GW_WAN_SIG_PUB_PRE (Key.WAN_SIG_PRE).
Klassifizierung	Gutfall-Test

3.28.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.28.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.28.4 APDU-Kommandos

ID: CM-Funktion_IFO_7b_4						
CLA	INS	P1	P2	Lc	Data	Le
00	22	41	b6	0f	80 0a [09 04 00 7f 00 07 01 01 04 01] 83 01 [02]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

3.28.5 Erwartete Ergebnisse

ID	Beschreibung
RS-DAEA	Das Key-Objekt 'Key.WAN_SIG_PRE' ist vorhanden.

3.29 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_7b_5)

3.29.1 Informationen

ID	TC_Funktion_IFO_7b_5
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im DF.SMGW des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des MSE-Set-Kommandos, ob alle Key-Pair-Objekte für DST im DF.SMGW des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Key Pair-Objekt für GW-Betriebsschlüsselpaar bzgl. TLS, also (GW_WAN_TLS_PRV, GW_WAN_TLS_PUB) (Key.WAN_TLS).
Klassifizierung	Gutfall-Test

3.29.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.29.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.29.4 APDU-Kommandos

ID: CM-Funktion_IFO_7b_5							
CLA	INS	P1	P2	Lc	Data	Le	
00	22	41	b6	0f	80 0a [09 04 00 7f 00 07 01 01 04 01] 83 01	--	

					[04]	

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

3.29.5 Erwartete Ergebnisse

ID	Beschreibung
RS-42E5	Das Key-Objekt 'Key.WAN_TLS' ist vorhanden.

3.30 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_7b_6)

3.30.1 Informationen

ID	TC_Funktion_IFO_7b_6
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im DF.SMGW des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des MSE-Set-Kommandos, ob alle Key-Pair-Objekte für DST im DF.SMGW des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Key Pair-Objekt für GW-Betriebsschlüsselpaar bzgl. SIG, also (GW_WAN_SIG_PRV, GW_WAN_SIG_PUB) (Key.WAN_SIG).
Klassifizierung	Gutfall-Test

3.30.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.30.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.30.4 APDU-Kommandos

ID: CM-Funktion_IFO_7b_6

CLA	INS	P1	P2	Lc	Data	Le
00	22	41	b6	0f	80 0a [09 04 00 7f 00 07 01 01 04 01] 83 01 [05]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

3.30.5 Erwartete Ergebnisse

ID	Beschreibung
RS-4A84	Das Key-Objekt 'Key.WAN_SIG' ist vorhanden.

3.31 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_7c_7)

3.31.1 Informationen

ID	TC_Funktion_IFO_7c_7
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im DF.SMGW des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des MSE-Set-Kommandos, ob alle Key-Pair-Objekte für AT im DF.SMGW des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Key Pair-Objekt für vorläufiges GW-Schlüsselpaar bzgl. ENC, also (GW_WAN_ENC_PRV_PRE, GW_WAN_ENC_PUB_PRE) (Key.WAN_ENC_PRE).
Klassifizierung	Gutfall-Test

3.31.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.31.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.31.4 APDU-Kommandos

ID: CM-Funktion_IFO_7c_7						
CLA	INS	P1	P2	Lc	Data	Le
00	22	41	a4	0f	80 0a [09 04 00 7f 00 07 01 01 04 01] 84 01 [03]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '84-01-Key Reference' (für das Key Pair-Objekt)

3.31.5 Erwartete Ergebnisse

ID	Beschreibung
RS-2FC8	Das Key-Objekt 'Key.WAN_ENC_PRE' ist vorhanden.

3.32 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_7c_8)

3.32.1 Informationen

ID	TC_Funktion_IFO_7c_8
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im DF.SMGW des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des MSE-Set-Kommandos, ob alle Key-Pair-Objekte für AT im DF.SMGW des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Key Pair-Objekt für GW-Betriebsschlüsselpaar bzgl. ENC, also (GW_WAN_ENC_PRV, GW_WAN_ENC_PUB (Key.WAN_ENC)).
Klassifizierung	Gutfall-Test

3.32.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.32.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.32.4 APDU-Kommandos

ID: CM-Funktion_IFO_7c_8							
CLA	INS	P1	P2	Lc	Data	Le	
00	22	41	a4	0f	80 0a [09 04 00 7f 00 07 01 01 04 01] 84 01 [06]	--	

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '84-01-Key Reference' (für das Key Pair-Objekt)

3.32.5 Erwartete Ergebnisse

ID	Beschreibung
RS-DCEA	Das Key-Objekt 'Key.WAN_ENC' ist vorhanden.

3.33 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_7c_9)

3.33.1 Informationen

ID	TC_Funktion_IFO_7c_9
Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im DF.SMGW des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des MSE-Set-Kommandos, ob alle Key-Pair-Objekte für AT im DF.SMGW des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Key Pair-Objekt für ephemerales Schlüsselpaar des GW im Rahmen von ECKA-DH, also (GW_PRV_EPH, GW_PUB_EPH) (Key.EPH_1).
Klassifizierung	Gutfall-Test

3.33.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.33.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.33.4 APDU-Kommandos

ID: CM-Funktion_IFO_7c_9						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	10	80 0b [0a 04 00 7f 00 07 02 02 0a 02 01] 84 01 [7e]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

3.33.5 Erwartete Ergebnisse

ID	Beschreibung
RS-7736	Das Key-Objekt 'Key.EPH_1' ist vorhanden.

3.34 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_7c_10)

3.34.1 Informationen

ID	TC_Funktion_IFO_7c_10

Beschreibung	Es wird getestet, ob bestimmte Dateien und Objekte im DF.SMGW des initialen Dateisystems vorhanden sind. Der Testfall prüft mittels des MSE-Set-Kommandos, ob alle Key-Pair-Objekte für AT im DF.SMGW des initialen Dateisystems vorhanden sind. Die Durchführung erfolgt für das Key Pair-Objekt für ephemerales Schlüsselpaar des GW im Rahmen von ECKA-DH, also (GW_PRV_EPH, GW_PUB_EPH) (Key.EPH_2).
Klassifizierung	Gutfall-Test

3.34.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.34.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.34.4 APDU-Kommandos

ID: CM-Funktion_IFO_7c_10						
CLA	INS	P1	P2	Lc	Data	Le
00	22	c1	a4	10	80 0b [0a 04 00 7f 00 07 02 02 0a 02 01] 84 01 [7f]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') || '83-L83-Key Reference' (für das Public Key-Objekt) || '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' || '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' || '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)

3.34.5 Erwartete Ergebnisse

ID	Beschreibung
RS-F8AD	Das Key-Objekt 'Key.EPH_2' ist vorhanden.

3.35 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_11_1)

3.35.1 Informationen

ID	TC_Funktion_IFO_11_1
Beschreibung	Es wird getestet, ob sich initiale Dateien personalisieren lassen. Dieser Testfall prüft das File EF.SECModTRInfo auf korrekten Inhalt (Technische Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation - insbesondere Angabe der Version der vorliegenden TR, auf Basis derer das vorliegende Sicherheitsmodul implementiert wurde).
Klassifizierung	Gutfall-Test

3.35.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.35.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.35.4 APDU-Kommandos

ID: CM-Funktion_IFO_11_1						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	02	0c	02	01 1a	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

ID: CM-Funktion_IFO_11_1

CLA	INS	P1	P2	Lc	Data	Le
00	b2	LL	04	--	--	XX... XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.35.5 Erwartete Ergebnisse

ID	Beschreibung
RS-D538	Das Testsystem antwortet mit den APDUs, die einen Erfolg der abgesetzten Kommandos bedeuten, und der Inhalt des EFs muss den Vorgaben entsprechen

3.36 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_12_2)

3.36.1 Informationen

ID	TC_Funktion_IFO_12_2
Beschreibung	Es wird getestet, ob sich initiale Dateien personalisieren lassen. Dieser Testfall prüft das File EF.SecModAccess auf korrekten Inhalt (Korrekte Codierung der Information zur PACE-Codierung nach TR-03110-3).
Klassifizierung	Gutfall-Test

3.36.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.36.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.36.4 APDU-Kommandos

ID: CM-Funktion_IFO_12_2						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	02	0c	02	01 1b	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

ID: CM-Funktion_IFO_12_2						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	LL	LL	--	--	XX... XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.36.5 Erwartete Ergebnisse

ID	Beschreibung
RS-D538	Das Testsystem antwortet mit den APDUs, die einen Erfolg der abgesetzten Kommandos bedeuten, und der Inhalt des EFs muss den Vorgaben entsprechen

3.37 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_13_3)

3.37.1 Informationen

ID	TC_Funktion_IFO_13_3
Beschreibung	Es wird getestet, ob sich initiale Dateien personalisieren lassen. Dieser Testfall prüft das File EF.SecModCrypto auf korrekten Inhalt (Korrekte Codierung der Krypto-Informationen).
Klassifizierung	Gutfall-Test

3.37.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.37.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.37.4 APDU-Kommandos

ID: CM-Funktion_IFO_13_3						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	02	0c	02	01 1c	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

ID: CM-Funktion_IFO_13_3						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	LL	LL	--	--	XX... XX

'P1' enthält $(\text{Offset} - \text{P2}) / 256$, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.37.5 Erwartete Ergebnisse

ID	Beschreibung
RS-D538	Das Testsystem antwortet mit den APDUs, die einen Erfolg der abgesetzten Kommandos bedeuten, und der Inhalt des EFs muss den Vorgaben entsprechen

3.38 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_9a_1)

3.38.1 Informationen

ID	TC_Funktion_IFO_9a_1
Beschreibung	Es wird getestet, ob sich Schlüssel im MF und DF.SMGW personalisieren lassen. Dieser Testfall prüft implizit über kryptographische Kommandos nach TR-03109-2, Tabelle 17, ob sich Key-Objekte für DST im MF des initialen Filesystem korrekt mit Schlüsseln "befüllen" und sich die Schlüssel anschließend korrekt gemäß der Vorbelegung nach TR-03109-2, Tabelle 4 verwenden lassen. Die Durchführung erfolgt für das Public Key-Objekt für GW-Admin-Schlüssel bzgl. TLS, also GWADM_TLS_PUB (Key.GWA_TLS_1).
Klassifizierung	Gutfall-Test

3.38.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.38.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.38.4 APDU-Kommandos

ID: CM-Funktion_IFO_9a_1						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	1e	62 1c [ad 1a [83 04 [00 00 00 11] 96 00 a2 00 7b 0e [b6 0c [80 0a [09 04 00 7f 00 07 01 01 04 01]]]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.38.5 Erwartete Ergebnisse

ID	Beschreibung
RS-12BA	Das Key-Objekt 'Key.GWA_TLS_1' lässt sich korrekt befüllen und auslesen.

3.39 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_9a_2)

3.39.1 Informationen

ID	TC_Funktion_IFO_9a_2
Beschreibung	Es wird getestet, ob sich Schlüssel im MF und DF.SMGW personalisieren lassen. Dieser Testfall prüft implizit über kryptographische Kommandos nach TR-03109-2, Tabelle 17, ob sich Key-Objekte für DST im MF des initialen Filesystem korrekt mit Schlüsseln "befüllen" und sich die Schlüssel anschließend korrekt gemäß der Vorbelegung nach TR-03109-2, Tabelle 4 verwenden lassen. Die Durchführung erfolgt für das Public Key-Objekt für GW-Admin-Schlüssel bzgl. SIG, also GWADM_SIG_PUB (Key.GWA_SIG_1).
Klassifizierung	Gutfall-Test

3.39.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.39.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.39.4 APDU-Kommandos

ID: CM-Funktion_IFO_9a_2						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	1e	62 1c [ad 1a [83 04 [00 00 00 12] 96 00 a2 00	--

					7b 0e [b6 0c [80 0a [09 04 00 7f 00 07 01 01 04 01]]]]]	

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.39.5 Erwartete Ergebnisse

ID	Beschreibung
RS-8C0F	Das Key-Objekt 'Key.GWA_SIG_1' lässt sich korrekt befüllen und auslesen.

3.40 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_9a_3)

3.40.1 Informationen

ID	TC_Funktion_IFO_9a_3
Beschreibung	Es wird getestet, ob sich Schlüssel im MF und DF.SMGW personalisieren lassen. Dieser Testfall prüft implizit über kryptographische Kommandos nach TR-03109-2, Tabelle 17, ob sich Key-Objekte für DST im MF des initialen Filesystem korrekt mit Schlüsseln "befüllen" und sich die Schlüssel anschließend korrekt gemäß der Vorbelegung nach TR-03109-2, Tabelle 4 verwenden lassen. Die Durchführung erfolgt für das Public Key-Objekt für GW-Admin-Schlüssel bzgl. TLS, also GWADM_TLS_PUB (Key.GWA_TLS_2.).
Klassifizierung	Gutfall-Test

3.40.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.40.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.40.4 APDU-Kommandos

ID: CM-Funktion_IFO_9a_3						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	1e	62 1c [ad 1a [83 04 [00 00 00 21] 96 00 a2 00 7b 0e [b6 0c [80 0a [09 04 00 7f 00 07 01 01 04 01]]]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.40.5 Erwartete Ergebnisse

ID	Beschreibung
RS-4746	Das Key-Objekt 'Key.GWA_TLS_2).' lässt sich korrekt befüllen und auslesen.

3.41 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_9a_4)

3.41.1 Informationen

ID	TC_Funktion_IFO_9a_4
Beschreibung	Es wird getestet, ob sich Schlüssel im MF und DF.SMGW personalisieren lassen. Dieser Testfall prüft implizit über kryptographische Kommandos nach TR-03109-2, Tabelle 17, ob sich Key-Objekte für DST im MF des initialen Filesystem korrekt mit Schlüsseln "befüllen" und sich die Schlüssel anschließend korrekt gemäß der Vorbelegung nach TR-03109-2, Tabelle 4 verwenden lassen. Die Durchführung erfolgt für das Public Key-Objekt für GW-Admin-Schlüssel bzgl. SIG, also GWADM_SIG_PUB (Key.GWA_SIG_2).
Klassifizierung	Gutfall-Test

3.41.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.41.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.41.4 APDU-Kommandos

ID: CM-Funktion_IFO_9a_4						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	1e	62 1c [ad 1a [83 04 [00 00 00 22] 96 00 a2 00 7b 0e [b6 0c [80 0a [09 04 00 7f 00 07 01 01 04 01]]]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.41.5 Erwartete Ergebnisse

ID	Beschreibung
RS-DE7F	Das Key-Objekt 'Key.GWA_SIG_2' lässt sich korrekt befüllen und auslesen.

3.42 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_9a_5)

3.42.1 Informationen

ID	TC_Funktion_IFO_9a_5
Beschreibung	Es wird getestet, ob sich Schlüssel im MF und DF.SMGW personalisieren lassen. Dieser Testfall prüft implizit über kryptographische Kommandos nach TR-03109-2, Tabelle 17, ob sich Key-Objekte für DST im MF des initialen Filesystem korrekt mit Schlüsseln "befüllen" und sich die Schlüssel anschließend korrekt gemäß der Vorbelegung nach TR-03109-2, Tabelle 4 verwenden lassen. Die Durchführung erfolgt für das Public Key-Objekt für Transport-Import-Schlüssel, also IMP_PUB_TRANS (Key.IMP_PUB_TRANS).

Klassifizierung	Gutfall-Test

3.42.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.42.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.42.4 APDU-Kommandos

ID: CM-Funktion_IFO_9a_5						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	62 LL [ad LL [83 04 [00 00 00 31] 96 LL [XX...XX] a2 00 7b 0f [b6 0d [80 0b [0a 04 00 7f 00 07 01 01 04 04 03]]]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.42.5 Erwartete Ergebnisse

ID	Beschreibung
RS-C349	Das Key-Objekt 'Key.IMP_PUB_TRANS' lässt sich korrekt befüllen und auslesen.

3.43 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_9a_6)

3.43.1 Informationen

ID	TC_Funktion_IFO_9a_6

Beschreibung	Es wird getestet, ob sich Schlüssel im MF und DF.SMGW personalisieren lassen. Dieser Testfall prüft implizit über kryptographische Kommandos nach TR-03109-2, Tabelle 17, ob sich Key-Objekte für DST im MF des initialen Filesystem korrekt mit Schlüsseln "befüllen" und sich die Schlüssel anschließend korrekt gemäß der Vorbelegung nach TR-03109-2, Tabelle 4 verwenden lassen. Die Durchführung erfolgt für das Public Key-Objekt für Import-Schlüssel (Integrator-spezifisch), also IMP_PUB (Key.IMP_PUB).
Klassifizierung	Gutfall-Test

3.43.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.43.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.43.4 APDU-Kommandos

ID: CM-Funktion_IFO_9a_6						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	62 LL [ad LL [83 04 [00 00 00 32] 96 LL [XX...XX] a2 00 7b 0f [b6 0d [80 0b [0a 04 00 7f 00 07 01 01 04 04 03]]]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.43.5 Erwartete Ergebnisse

ID	Beschreibung
RS-1A15	Das Key-Objekt 'Key.IMP_PUB' lässt sich korrekt befüllen und auslesen.

3.44 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_9b_7)

3.44.1 Informationen

ID	TC_Funktion_IFO_9b_7
Beschreibung	Es wird getestet, ob sich Schlüssel im MF und DF.SMGW personalisieren lassen. Dieser Testfall prüft implizit über kryptographische Kommandos nach TR-03109-2, Tabelle 17, ob sich Key-Objekte für DST im MF des initialen Filesystem korrekt mit Schlüsseln "befüllen" und sich die Schlüssel anschließend korrekt gemäß der Vorbelegung nach TR-03109-2, Tabelle 4 verwenden lassen. Die Durchführung erfolgt für das Key Pair-Objekt für Transport-Import-Schlüsselpaar, also (IMP_PRV_TRANS, IMP_PUB_TRANS) (Key.IMP_TRANS).
Klassifizierung	Gutfall-Test

3.44.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.44.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.44.4 APDU-Kommandos

ID: CM-Funktion_IFO_9b_7						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	62 LL [ad LL [83 01 [31] 96 LL [XX...XX] a2 00 7b 0e [b6 0c [80 0a [09 04 00 7f 00 07 01 01 04 01]]]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.44.5 Erwartete Ergebnisse

ID	Beschreibung
RS-1EEB	Das Key-Objekt 'Key.IMP_TRANS' lässt sich korrekt befüllen und auslesen.

3.45 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_9b_8)

3.45.1 Informationen

ID	TC_Funktion_IFO_9b_8
Beschreibung	Es wird getestet, ob sich Schlüssel im MF und DF.SMGW personalisieren lassen. Dieser Testfall prüft implizit über kryptographische Kommandos nach TR-03109-2, Tabelle 17, ob sich Key-Objekte für DST im MF des initialen Filesystem korrekt mit Schlüsseln "befüllen" und sich die Schlüssel anschließend korrekt gemäß der Vorbelegung nach TR-03109-2, Tabelle 4 verwenden lassen. Die Durchführung erfolgt für das Key Pair-Objekt für Import-Schlüsselpaar (Integrator-spezifisch), also (IMP_PRV, IMP_PUB) ((Key.IMP).).
Klassifizierung	Gutfall-Test

3.45.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.45.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.45.4 APDU-Kommandos

ID: CM-Funktion_IFO_9b_8						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	62 LL [ad LL [83 01 [32] 96 LL [XX...XX]	--

					a2 00 7b 0e [b6 0c [80 0a [09 04 00 7f 00 07 01 01 04 01]]]]]	

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.45.5 Erwartete Ergebnisse

ID	Beschreibung
RS-0E00	Das Key-Objekt '(Key.IMP).' lässt sich korrekt befüllen und auslesen.

3.46 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_9c_9)

3.46.1 Informationen

ID	TC_Funktion_IFO_9c_9
Beschreibung	Es wird getestet, ob sich Schlüssel im MF und DF.SMGW personalisieren lassen. Dieser Testfall prüft implizit über kryptographische Kommandos nach TR-03109-2, Tabelle 17, ob sich Key-Objekte für AT im MF des initialen Filesystem korrekt mit Schlüsseln "befüllen" und sich die Schlüssel anschließend korrekt gemäß der Vorbelegung nach TR-03109-2, Tabelle 4 verwenden lassen. Die Durchführung erfolgt für das Public Key-Objekt für GW-Admin-Schlüssel bzgl. ENC, also GWADM_ENC_PUB (Key.GWA_ENC_1).
Klassifizierung	Gutfall-Test

3.46.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.46.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.46.4 APDU-Kommandos

ID: CM-Funktion_IFO_9c_9						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	1e	62 1c [ad 1a [83 04 [00 00 00 13] 96 00 a2 00 7b 0e [a4 0c [80 0a [09 04 00 7f 00 07 01 01 05 01]]]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.46.5 Erwartete Ergebnisse

ID	Beschreibung
RS-A60E	Das Key-Objekt 'Key.GWA_ENC_1' lässt sich korrekt befüllen und auslesen.

3.47 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_9c_10)

3.47.1 Informationen

ID	TC_Funktion_IFO_9c_10
Beschreibung	Es wird getestet, ob sich Schlüssel im MF und DF.SMGW personalisieren lassen. Dieser Testfall prüft implizit über kryptographische Kommandos nach TR-03109-2, Tabelle 17, ob sich Key-Objekte für AT im MF des initialen Filesystem korrekt mit Schlüsseln "befüllen" und sich die Schlüssel anschließend korrekt gemäß der Vorbelegung nach TR-03109-2, Tabelle 4 verwenden lassen. Die Durchführung erfolgt für das Public Key-Objekt für GW-Admin-Schlüssel bzgl. AUT, also GWADM_AUT_PUB (Key.GWA_AUT_1).
Klassifizierung	Gutfall-Test

3.47.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.47.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.47.4 APDU-Kommandos

ID: CM-Funktion_IFO_9c_10						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	1f	62 1d [ad 1b [83 04 [00 00 00 10] 96 00 a2 00 7b 0f [a4 0d [80 0b [0a 04 00 7f 00 07 01 01 04 01 03]]]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.47.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9C95	Das Key-Objekt 'Key.GWA_AUT_1' lässt sich korrekt befüllen und auslesen.

3.48 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_9c_11)

3.48.1 Informationen

ID	TC_Funktion_IFO_9c_11
Beschreibung	Es wird getestet, ob sich Schlüssel im MF und DF.SMGW personalisieren lassen. Dieser Testfall prüft implizit über kryptographische Kommandos nach TR-03109-2, Tabelle 17, ob sich Key-Objekte für AT im MF des initialen Filesystem korrekt mit Schlüsseln "befüllen" und sich die Schlüssel anschließend korrekt gemäß der Vorbelegung nach TR-03109-2, Tabelle 4 verwenden lassen. Die Durchführung erfolgt für das Public Key-Objekt für GW-Admin-Schlüssel bzgl. ENC, also GWADM_ENC_PUB (Key.GWA_ENC_2).

Klassifizierung	Gutfall-Test

3.48.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.48.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.48.4 APDU-Kommandos

ID: CM-Funktion_IFO_9c_11						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	1e	62 1c [ad 1a [83 04 [00 00 00 23] 96 00 a2 00 7b 0e [a4 0c [80 0a [09 04 00 7f 00 07 01 01 05 01]]]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.48.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6662	Das Key-Objekt 'Key.GWA_ENC_2' lässt sich korrekt befüllen und auslesen.

3.49 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_9c_12)

3.49.1 Informationen

ID	TC_Funktion_IFO_9c_12

Beschreibung	Es wird getestet, ob sich Schlüssel im MF und DF.SMGW personalisieren lassen. Dieser Testfall prüft implizit über kryptographische Kommandos nach TR-03109-2, Tabelle 17, ob sich Key-Objekte für AT im MF des initialen Filesystem korrekt mit Schlüsseln "befüllen" und sich die Schlüssel anschließend korrekt gemäß der Vorbelegung nach TR-03109-2, Tabelle 4 verwenden lassen. Die Durchführung erfolgt für das Public Key-Objekt für GW-Admin-Schlüssel bzgl. AUT, also GWADM_AUT_PUB. (Key.GWA_AUT_2).
Klassifizierung	Gutfall-Test

3.49.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.49.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.49.4 APDU-Kommandos

ID: CM-Funktion_IFO_9c_12						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	1f	62 1d [ad 1b [83 04 [00 00 00 20] 96 00 a2 00 7b 0f [a4 0d [80 0b [0a 04 00 7f 00 07 01 01 04 01 03]]]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.49.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9984	Das Key-Objekt 'Key.GWA_AUT_2' lässt sich korrekt befüllen und auslesen.

3.50 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_10a_13)

3.50.1 Informationen

ID	TC_Funktion_IFO_10a_13
Beschreibung	Es wird getestet, ob sich Schlüssel im MF und DF.SMGW personalisieren lassen. Dieser Testfall prüft implizit über kryptographische Kommandos nach TR-03109-2, Tabelle 17, ob sich Key-Objekte für DST im DF.SMGW des initialen Filesystem korrekt mit Schlüsseln "befüllen" und sich die Schlüssel anschließend korrekt gemäß der Vorbelegung nach TR-03109-2, Tabelle 4 verwenden lassen. Die Durchführung erfolgt für das Public-Key-Objekt für die SM-PKI-Root-Keys (Key.SMPKIRoot_x).
Klassifizierung	Gutfall-Test

3.50.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.50.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.50.4 APDU-Kommandos

ID: CM-Funktion_IFO_10a_13						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	1e	62 1c [ad 1a [83 04 [00 00 00 XX] 96 00 a2 00 7b 0e [b6 0c [80 0a [09 04 00 7f 00 07 01 01 04 01]]]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.50.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9571	Das Key-Objekt 'Key.SMPKIRoot_x' lässt sich korrekt befüllen und auslesen.

3.51 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_10a_14)

3.51.1 Informationen

ID	TC_Funktion_IFO_10a_14
Beschreibung	Es wird getestet, ob sich Schlüssel im MF und DF.SMGW personalisieren lassen. Dieser Testfall prüft implizit über kryptographische Kommandos nach TR-03109-2, Tabelle 17, ob sich Key-Objekte für DST im DF.SMGW des initialen Filesystem korrekt mit Schlüsseln "befüllen" und sich die Schlüssel anschließend korrekt gemäß der Vorbelegung nach TR-03109-2, Tabelle 4 verwenden lassen. Die Durchführung erfolgt für das Public-Key-Objekte für CA-Public Key (relevant für die Prüfung von Zertifikatsketten im Rahmen der SM-PKI) (Key.CA_x).
Klassifizierung	Gutfall-Test

3.51.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.51.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.51.4 APDU-Kommandos

ID: CM-Funktion_IFO_10a_14						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	1e	62 1c [ad 1a [83 04 [00 00 10 XX] 96 00 a2	--

					00 7b 0e [b6 0c [80 0a [09 04 00 7f 00 07 01 01 04 01]]]]]	

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.51.5 Erwartete Ergebnisse

ID	Beschreibung
RS-8B05	Das Key-Objekt 'Key.CA_x' lässt sich korrekt befüllen und auslesen.

3.52 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_10b_15)

3.52.1 Informationen

ID	TC_Funktion_IFO_10b_15
Beschreibung	Es wird getestet, ob sich Schlüssel im MF und DF.SMGW personalisieren lassen. Dieser Testfall prüft implizit über kryptographische Kommandos nach TR-03109-2, Tabelle 17, ob sich Key-Objekte für DST im DF.SMGW des initialen Filesystem korrekt mit Schlüsseln "befüllen" und sich die Schlüssel anschließend korrekt gemäß der Vorbelegung nach TR-03109-2, Tabelle 4 verwenden lassen. Die Durchführung erfolgt für das Key Pair-Objekt für vorläufiges GW-Schlüsselpaar bzgl. TLS, also (GW_WAN_TLS_PRV_PRE, GW_WAN_TLS_PUB_PRE (Key.WAN_TLS_PRE)).
Klassifizierung	Gutfall-Test

3.52.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.52.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.52.4 APDU-Kommandos

ID: CM-Funktion_IFO_10b_15						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	19	62 17 [ad LL [83 01 [01] 96 00 a1 00 7b 0e [b6 0c [80 0a [09 04 00 7f 00 07 01 01 04 01]]]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.52.5 Erwartete Ergebnisse

ID	Beschreibung
RS-BCAA	Das Key-Objekt 'Key.WAN_TLS_PRE' lässt sich korrekt befüllen und auslesen.

3.53 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_10b_16)

3.53.1 Informationen

ID	TC_Funktion_IFO_10b_16
Beschreibung	Es wird getestet, ob sich Schlüssel im MF und DF.SMGW personalisieren lassen. Dieser Testfall prüft implizit über kryptographische Kommandos nach TR-03109-2, Tabelle 17, ob sich Key-Objekte für DST im DF.SMGW des initialen Filesystem korrekt mit Schlüsseln "befüllen" und sich die Schlüssel anschließend korrekt gemäß der Vorbelegung nach TR-03109-2, Tabelle 4 verwenden lassen. Die Durchführung erfolgt für das Key Pair-Objekt für vorläufiges GW-Schlüsselpaar bzgl. TLS, also (GW_WAN_TLS_PRV_PRE, GW_WAN_TLS_PUB_PRE (Key.WAN_TLS_PRE)).
Klassifizierung	Gutfall-Test

3.53.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.53.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.53.4 APDU-Kommandos

ID: CM-Funktion_IFO_10b_16						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	19	62 17 [ad 15 [83 01 [02] 96 00 a1 00 7b 0e [b6 0c [80 0a [09 04 00 7f 00 07 01 01 04 01]]]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.53.5 Erwartete Ergebnisse

ID	Beschreibung
RS-BCAA	Das Key-Objekt 'Key.WAN_TLS_PRE' lässt sich korrekt befüllen und auslesen.

3.54 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_10b_17)

3.54.1 Informationen

ID	TC_Funktion_IFO_10b_17
Beschreibung	Es wird getestet, ob sich Schlüssel im MF und DF.SMGW personalisieren lassen. Dieser Testfall prüft implizit über kryptographische Kommandos nach TR-03109-2, Tabelle 17, ob sich Key-Objekte für DST im

	DF.SMGW des initialen Filesystem korrekt mit Schlüsseln "befüllen" und sich die Schlüssel anschließend korrekt gemäß der Vorbelegung nach TR-03109-2, Tabelle 4 verwenden lassen. Die Durchführung erfolgt für das Key Pair-Objekt für GW-Betriebsschlüsselpaar bzgl. TLS, also (GW_WAN_TLS_PRV, GW_WAN_TLS_PUB) (Key.WAN_TLS).
Klassifizierung	Gutfall-Test

3.54.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.54.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.54.4 APDU-Kommandos

ID: CM-Funktion_IFO_10b_17						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	19	62 17 [ad 15 [83 01 [04] 96 00 a1 00 7b 0e [b6 0c [80 0a [09 04 00 7f 00 07 01 01 04 01]]]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.54.5 Erwartete Ergebnisse

ID	Beschreibung
RS-F9E5	Das Key-Objekt 'Key.WAN_TLS' lässt sich korrekt befüllen und auslesen.

3.55 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_10b_18)

3.55.1 Informationen

ID	TC_Funktion_IFO_10b_18
Beschreibung	Es wird getestet, ob sich Schlüssel im MF und DF.SMGW personalisieren lassen. Dieser Testfall prüft implizit über kryptographische Kommandos nach TR-03109-2, Tabelle 17, ob sich Key-Objekte für DST im DF.SMGW des initialen Filesystem korrekt mit Schlüsseln "befüllen" und sich die Schlüssel anschließend korrekt gemäß der Vorbelegung nach TR-03109-2, Tabelle 4 verwenden lassen. Die Durchführung erfolgt für das Key Pair-Objekt für GW-Betriebsschlüsselpaar bzgl. SIG, also (GW_WAN_SIG_PRV, GW_WAN_SIG_PUB) (Key.WAN_SIG).
Klassifizierung	Gutfall-Test

3.55.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.55.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.55.4 APDU-Kommandos

ID: CM-Funktion_IFO_10b_18						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	19	62 17 [ad 15 [83 01 [05] 96 00 a1 00 7b 0e [b6 0c [80 0a [09 04 00 7f 00 07 01 01 04 01]]]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.55.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6C4E	Das Key-Objekt 'Key.WAN_SIG' lässt sich korrekt befüllen und auslesen.

3.56 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_10c_19)

3.56.1 Informationen

ID	TC_Funktion_IFO_10c_19
Beschreibung	Es wird getestet, ob sich Schlüssel im MF und DF.SMGW personalisieren lassen. Dieser Testfall prüft implizit über kryptographische Kommandos nach TR-03109-2, Tabelle 17, ob sich Key-Objekte für AT im DF.SMGW des initialen Filesystem korrekt mit Schlüsseln "befüllen" und sich die Schlüssel anschließend korrekt gemäß der Vorbelegung nach TR-03109-2, Tabelle 4 verwenden lassen. Die Durchführung erfolgt für das Key Pair-Objekt für vorläufiges GW-Schlüsselpaar bzgl. ENC, also (GW_WAN_ENC_PRV_PRE, GW_WAN_ENC_PUB_PRE) (Key.WAN_ENC_PRE).
Klassifizierung	Gutfall-Test

3.56.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.56.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.56.4 APDU-Kommandos

ID: CM-Funktion_IFO_10c_19						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	19	62 17 [ad 15 [83 01 [03] 96 00 a1 00 7b 0e	--

					[a4 0c [80 0a [09 04 00 7f 00 07 01 01 04 01]]]]]	

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.56.5 Erwartete Ergebnisse

ID	Beschreibung
RS-4CDE	Das Key-Objekt 'Key.WAN_ENC_PRE' lässt sich korrekt befüllen und auslesen.

3.57 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_10c_20)

3.57.1 Informationen

ID	TC_Funktion_IFO_10c_20
Beschreibung	Es wird getestet, ob sich Schlüssel im MF und DF.SMGW personalisieren lassen. Dieser Testfall prüft implizit über kryptographische Kommandos nach TR-03109-2, Tabelle 17, ob sich Key-Objekte für AT im DF.SMGW des initialen Filesystem korrekt mit Schlüsseln "befüllen" und sich die Schlüssel anschließend korrekt gemäß der Vorbelegung nach TR-03109-2, Tabelle 4 verwenden lassen. Die Durchführung erfolgt für das Key Pair-Objekt für GW-Betriebsschlüsselpaar bzgl. ENC, also (GW_WAN_ENC_PRV, GW_WAN_ENC_PUB (Key.WAN_ENC)).
Klassifizierung	Gutfall-Test

3.57.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.57.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.57.4 APDU-Kommandos

ID: CM-Funktion_IFO_10c_20						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	19	62 17 [ad 15 [83 01 [06] 96 00 a1 00 7b 0e [a4 0c [80 0a [09 04 00 7f 00 07 01 01 04 01]]]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.57.5 Erwartete Ergebnisse

ID	Beschreibung
RS-162D	Das Key-Objekt 'Key.WAN_ENC' lässt sich korrekt befüllen und auslesen.

3.58 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_10c_21)

3.58.1 Informationen

ID	TC_Funktion_IFO_10c_21
Beschreibung	Es wird getestet, ob sich Schlüssel im MF und DF.SMGW personalisieren lassen. Dieser Testfall prüft implizit über kryptographische Kommandos nach TR-03109-2, Tabelle 17, ob sich Key-Objekte für AT im DF.SMGW des initialen Filesystem korrekt mit Schlüsseln "befüllen" und sich die Schlüssel anschließend korrekt gemäß der Vorbelegung nach TR-03109-2, Tabelle 4 verwenden lassen. Die Durchführung erfolgt für das Key Pair-Objekt für ephemerales Schlüsselpaar des GW im Rahmen von ECKA-DH, also (GW_PRV_EPH, GW_PUB_EPH) (Key.EPH_1).
Klassifizierung	Gutfall-Test

3.58.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.58.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.58.4 APDU-Kommandos

ID: CM-Funktion_IFO_10c_21						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	19	62 17 [ad 15 [83 01 [7e] 96 00 a1 00 7b 0e [a4 0c [80 0a [09 04 00 7f 00 07 01 01 05 02]]]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.58.5 Erwartete Ergebnisse

ID	Beschreibung
RS-5377	Das Key-Objekt 'Key.EPH_1' lässt sich korrekt befüllen und auslesen.

3.59 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_10c_22)

3.59.1 Informationen

ID	TC_Funktion_IFO_10c_22
Beschreibung	Es wird getestet, ob sich Schlüssel im MF und DF.SMGW personalisieren lassen. Dieser Testfall prüft implizit über kryptographische Kommandos nach TR-03109-2, Tabelle 17, ob sich Key-Objekte für AT im DF.SMGW des initialen Filesystem korrekt mit Schlüsseln "befüllen" und sich die Schlüssel anschließend korrekt gemäß der Vorbelegung nach TR-03109-2, Tabelle 4 verwenden lassen. Die Durchführung erfolgt für das Key Pair-Objekt für ephemerales Schlüsselpaar des GW im Rahmen von ECKA-DH, also (GW_PRV_EPH, GW_PUB_EPH) (Key.EPH_2).

Klassifizierung	Gutfall-Test

3.59.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.1.2

3.59.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.59.4 APDU-Kommandos

ID: CM-Funktion_IFO_10c_22						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	19	62 17 [ad 15 [83 01 [7f] 96 00 a1 00 7b 0e [a4 0c [80 0a [09 04 00 7f 00 07 01 01 05 02]]]]]	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.59.5 Erwartete Ergebnisse

ID	Beschreibung
RS-3E73	Das Key-Objekt 'Key.EPH_2' lässt sich korrekt befüllen und auslesen.

3.60 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_1)

3.60.1 Informationen

ID	TC_Funktion_IFO_14_1
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien

	und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für MF, das Kommando 'CREATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.60.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.60.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.60.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_1 CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.60.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.61 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_2)

3.61.1 Informationen

ID	TC_Funktion_IFO_14_2
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für MF, das Kommando 'CREATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.61.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.61.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.61.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_2						
CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.61.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.62 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_3)

3.62.1 Informationen

ID	TC_Funktion_IFO_14_3
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für MF, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.62.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.62.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.62.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_3						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.62.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.63 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_4)

3.63.1 Informationen

ID	TC_Funktion_IFO_14_4
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für MF, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.63.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.63.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.63.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_4						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.63.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.64 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_5)

3.64.1 Informationen

ID	TC_Funktion_IFO_14_5
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für MF, das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.64.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.64.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.64.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_5						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le

00	04	00	00	--	--	--

3.64.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.65 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_6)

3.65.1 Informationen

ID	TC_Funktion_IFO_14_6
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für MF, das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.65.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.65.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.65.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_6 DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le

00	04	00	00	--	--	--

3.65.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.66 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_7)

3.66.1 Informationen

ID	TC_Funktion_IFO_14_7
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für MF, das Kommando 'DELETE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.66.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.66.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.66.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_7						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le

00	e4	00	00	--	--	--

3.66.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.67 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_8)

3.67.1 Informationen

ID	TC_Funktion_IFO_14_8
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für MF, das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.67.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.67.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.67.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_8						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le

00	e4	00	00	--	--	--

3.67.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.68 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_9)

3.68.1 Informationen

ID	TC_Funktion_IFO_14_9
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für MF, das Kommando 'SELECT (MF)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.68.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.68.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.68.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_9 SELECT (MF)						
CLA	INS	P1	P2	Lc	Data	Le

00	a4	00	0c	02	3f 00	--

3.68.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.69 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_10)

3.69.1 Informationen

ID	TC_Funktion_IFO_14_10
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für MF, das Kommando 'TERMINATE DF' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.69.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.69.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.69.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_10						
TERMINATE DF						
CLA	INS	P1	P2	Lc	Data	Le

00	e6	00	00	--	--	--

3.69.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.70 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_11)

3.70.1 Informationen

ID	TC_Funktion_IFO_14_11
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für MF, das Kommando 'TERMINATE DF' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.70.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.70.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.70.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_11						
TERMINATE DF						
CLA	INS	P1	P2	Lc	Data	Le

00	e6	00	00	--	--	--

3.70.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.71 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_12)

3.71.1 Informationen

ID	TC_Funktion_IFO_14_12
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'ACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.71.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.71.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.71.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_12 ACTIVATE FILE

CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.71.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.72 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_13)

3.72.1 Informationen

ID	TC_Funktion_IFO_14_13
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.72.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.72.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.72.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_13

ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.72.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.73 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_14)

3.73.1 Informationen

ID	TC_Funktion_IFO_14_14
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'APPEND RECORD (ohne SFI)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist. Dieser Testfall ist nur gültig, sofern das Kommando im Sicherheitsmodul implementiert ist
Klassifizierung	Gutfall-Test

3.73.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.73.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.73.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_14						
APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.73.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.74 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_15)

3.74.1 Informationen

ID	TC_Funktion_IFO_14_15
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.74.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.74.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.74.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_15						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.74.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.75 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_16)

3.75.1 Informationen

ID	TC_Funktion_IFO_14_16
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.75.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.75.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.75.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_16						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.75.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.76 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_17)

3.76.1 Informationen

ID	TC_Funktion_IFO_14_17
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'DELETE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.76.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.76.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.76.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_17						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.76.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.77 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_18)

3.77.1 Informationen

ID	TC_Funktion_IFO_14_18
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.77.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.77.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.77.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_18						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.77.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.78 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_19)

3.78.1 Informationen

ID	TC_Funktion_IFO_14_19
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'READ RECORD (ohne SFI)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.78.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.78.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.78.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_19 READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.78.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.79 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_20)

3.79.1 Informationen

ID	TC_Funktion_IFO_14_20
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'SELECT (EF mittels FID)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.79.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.79.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.79.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_20						
SELECT (EF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	02	0c	02	XX XX	--

'Data' enthält den File-Identifizierer des zu selektierenden EF.

3.79.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.80 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_21)

3.80.1 Informationen

ID	TC_Funktion_IFO_14_21
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'TERMINATE EF' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.80.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.80.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.80.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_21						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.80.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.81 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_22)

3.81.1 Informationen

ID	TC_Funktion_IFO_14_22
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'TERMINATE EF' und den

	Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.81.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.81.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.81.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_22						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.81.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.82 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_23)

3.82.1 Informationen

ID	TC_Funktion_IFO_14_23
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit

	Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'UPDATE RECORD (ohne SFI)' und ohne Sicherheitszustand. Dieser Testfall ist nur gültig, wenn das Sicherheitsmodul nicht die Funktionalität des Sicherheitsmodul-Firmware-Updates bietet (in diesem Fall gelten die Zugriffsregeln für ein Update des Datenfeldes wie im Rahmen des Firmware-Updates vorgesehen)
Klassifizierung	Fehlerfall-Test

3.82.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.82.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.82.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_23						
UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.82.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.83 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_24)

3.83.1 Informationen

ID	TC_Funktion_IFO_14_24
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'UPDATE RECORD (ohne SFI)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.83.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.83.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.83.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_24 UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.83.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.84 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_25)

3.84.1 Informationen

ID	TC_Funktion_IFO_14_25
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModAccess (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen PACE-Funktionalität), das Kommando 'READ BINARY (ohne SFI)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.84.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.84.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.84.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_25 READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält $(\text{Offset} - \text{P2}) / 256$, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.84.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.85 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_26)

3.85.1 Informationen

ID	TC_Funktion_IFO_14_26
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModAccess (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen PACE-Funktionalität), das Kommando 'SELECT (EF mittels FID)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.85.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.85.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.85.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_26

SELECT (EF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	02	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

3.85.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.86 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_27)

3.86.1 Informationen

ID	TC_Funktion_IFO_14_27
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModAccess (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen PACE-Funktionalität), das Kommando 'UPDATE BINARY (ohne SFI)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.86.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.86.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.86.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_27 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.86.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.87 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_28)

3.87.1 Informationen

ID	TC_Funktion_IFO_14_28
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModAccess (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen PACE-Funktionalität), das Kommando 'UPDATE BINARY (ohne SFI)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.87.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.87.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.87.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_28							
UPDATE BINARY (ohne SFI)							
CLA	INS	P1	P2	Lc	Data	Le	
00	d6	XX	XX	LL	XX...XX	--	

'P1' enthält $(\text{Offset} - \text{P2}) / 256$, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.87.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.88 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_29)

3.88.1 Informationen

ID	TC_Funktion_IFO_14_29
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität), das Kommando 'ACTIVATE FILE' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.88.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.88.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.88.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_29						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.88.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.89 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_30)

3.89.1 Informationen

ID	TC_Funktion_IFO_14_30
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität), das Kommando 'ACTIVATE FILE' und den

	Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.89.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.89.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.89.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_30						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.89.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.90 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_31)

3.90.1 Informationen

ID	TC_Funktion_IFO_14_31
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModCrypto (Technisches Datenfeld mit

	Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität), das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.90.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.90.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.90.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_31 DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.90.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.91 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_32)

3.91.1 Informationen

ID	TC_Funktion_IFO_14_32
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-

	Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität), das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.91.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.91.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.91.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_32						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.91.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.92 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_33)

3.92.1 Informationen

ID	TC_Funktion_IFO_14_33
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien

	und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität), das Kommando 'DELETE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.92.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.92.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.92.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_33						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.92.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.93 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_34)

3.93.1 Informationen

ID	TC_Funktion_IFO_14_34

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität), das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.93.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.93.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.93.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_34						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.93.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.94 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_35)

3.94.1 Informationen

ID	TC_Funktion_IFO_14_35
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität), das Kommando 'READ BINARY (ohne SFI)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.94.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.94.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.94.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_35 READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.94.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.95 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_36)

3.95.1 Informationen

ID	TC_Funktion_IFO_14_36
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität), das Kommando 'SELECT (EF mittels FID)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.95.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.95.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.95.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_36 SELECT (EF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	02	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

3.95.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.96 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_37)

3.96.1 Informationen

ID	TC_Funktion_IFO_14_37
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität), das Kommando 'TERMINATE EF' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.96.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.96.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.96.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_37							
TERMINATE EF							
CLA	INS	P1	P2	Lc	Data	Le	

00	e8	00	00	--	--	--

3.96.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.97 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_38)

3.97.1 Informationen

ID	TC_Funktion_IFO_14_38
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität), das Kommando 'TERMINATE EF' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.97.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.97.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.97.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_38 TERMINATE EF

CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.97.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.98 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_39)

3.98.1 Informationen

ID	TC_Funktion_IFO_14_39
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität), das Kommando 'UPDATE BINARY (ohne SFI)' und ohne Sicherheitszustand. Dieser Testfall ist nur gültig, wenn das Sicherheitsmodul nicht die Funktionalität des Sicherheitsmodul-Firmware-Updates bietet (in diesem Fall gelten die Zugriffsregeln für ein Update des Datenfeldes wie im Rahmen des Firmware-Updates vorgesehen)
Klassifizierung	Fehlerfall-Test

3.98.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.98.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.98.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_39						
UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.98.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.99 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_40)

3.99.1 Informationen

ID	TC_Funktion_IFO_14_40
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität), das Kommando 'UPDATE BINARY (ohne SFI)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.99.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.99.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.99.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_40 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält $(\text{Offset} - \text{P2}) / 256$, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.99.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.100 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_41)

3.100.1 Informationen

ID	TC_Funktion_IFO_14_41
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls), das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung

	von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.100.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.100.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.100.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_41						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.100.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.101 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_42)

3.101.1 Informationen

ID	TC_Funktion_IFO_14_42
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModLifeCycle (Technisches Datenfeld

	mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls), das Kommando 'APPEND RECORD (ohne SFI)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.101.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.101.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.101.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_42 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.101.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.102 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_43)

3.102.1 Informationen

ID	TC_Funktion_IFO_14_43
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls), das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.102.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.102.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.102.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_43						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.102.5 Erwartete Ergebnisse

ID	Beschreibung

RS-9000	Das Testsystem antwortet mit '90 00'.

3.103 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_44)

3.103.1 Informationen

ID	TC_Funktion_IFO_14_44
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls), das Kommando 'DELETE FILE' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.103.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.103.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.103.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_44 DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.103.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.104 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_45)

3.104.1 Informationen

ID	TC_Funktion_IFO_14_45
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls), das Kommando 'READ RECORD (ohne SFI)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.104.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.104.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.104.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_45 READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le

00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.104.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.105 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_46)

3.105.1 Informationen

ID	TC_Funktion_IFO_14_46
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls), das Kommando 'SELECT (EF mittels FID)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.105.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.105.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.105.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_46						
SELECT (EF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	02	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

3.105.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.106 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_47)

3.106.1 Informationen

ID	TC_Funktion_IFO_14_47
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls), das Kommando 'TERMINATE EF' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.106.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.106.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.106.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_47						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.106.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.107 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_48)

3.107.1 Informationen

ID	TC_Funktion_IFO_14_48
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls), das Kommando 'UPDATE RECORD (ohne SFI)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.107.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.107.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.107.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_48						
UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.107.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.108 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_49)

3.108.1 Informationen

ID	TC_Funktion_IFO_14_49
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.108.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.108.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.108.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_49						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.108.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.109 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_50)

3.109.1 Informationen

ID	TC_Funktion_IFO_14_50
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien

	und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.109.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.109.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.109.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_50						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.109.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.110 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_51)

3.110.1 Informationen

ID	TC_Funktion_IFO_14_51
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.110.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.110.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.110.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_51 CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.110.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.111 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_52)

3.111.1 Informationen

ID	TC_Funktion_IFO_14_52
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.111.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.111.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.111.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_52						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.111.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.112 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_53)

3.112.1 Informationen

ID	TC_Funktion_IFO_14_53
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.112.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.112.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.112.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_53

DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.112.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.113 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_54)

3.113.1 Informationen

ID	TC_Funktion_IFO_14_54
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.113.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.113.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.113.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_54						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.113.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.114 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_55)

3.114.1 Informationen

ID	TC_Funktion_IFO_14_55
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.114.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.114.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.114.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_55						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.114.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.115 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_56)

3.115.1 Informationen

ID	TC_Funktion_IFO_14_56
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.115.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.115.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.115.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_56 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.115.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.116 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_57)

3.116.1 Informationen

ID	TC_Funktion_IFO_14_57
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.

Klassifizierung	Fehlerfall-Test

3.116.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.116.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.116.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_57 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.116.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.117 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_58)

3.117.1 Informationen

ID	TC_Funktion_IFO_14_58
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die

	Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.117.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.117.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.117.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_58 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.117.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.118 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_59)

3.118.1 Informationen

ID	TC_Funktion_IFO_14_59
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.118.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.118.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.118.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_59 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve)

86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.118.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.119 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_60)

3.119.1 Informationen

ID	TC_Funktion_IFO_14_60
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.119.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.119.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.119.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_60
GENERAL AUTHENTICATE (ECKA-EG)

CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.119.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.120 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_61)

3.120.1 Informationen

ID	TC_Funktion_IFO_14_61
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.120.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.120.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.120.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_61						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.120.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.121 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_62)

3.121.1 Informationen

ID	TC_Funktion_IFO_14_62
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-

	Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.121.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.121.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.121.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_62 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.121.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.122 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_63)

3.122.1 Informationen

ID	TC_Funktion_IFO_14_63
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.122.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.122.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.122.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_63 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.122.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.123 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_64)

3.123.1 Informationen

ID	TC_Funktion_IFO_14_64
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.123.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.123.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.123.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_64 GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.123.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.124 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_65)

3.124.1 Informationen

ID	TC_Funktion_IFO_14_65
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.124.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.124.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.124.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_65
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.124.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.125 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_66)

3.125.1 Informationen

ID	TC_Funktion_IFO_14_66
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.125.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.125.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.125.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_66						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.125.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.126 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_67)

3.126.1 Informationen

ID	TC_Funktion_IFO_14_67
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.126.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.126.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.126.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_67						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.126.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.127 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_68)

3.127.1 Informationen

ID	TC_Funktion_IFO_14_68
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das

	MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.127.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.127.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.127.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_68						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.127.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.128 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_69)

3.128.1 Informationen

ID	TC_Funktion_IFO_14_69
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.128.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.128.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.128.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_69						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu

generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'
Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.128.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.129 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_70)

3.129.1 Informationen

ID	TC_Funktion_IFO_14_70
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.129.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.129.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.129.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_70 INTERNAL AUTHENTICATE

CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.129.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.130 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_71)

3.130.1 Informationen

ID	TC_Funktion_IFO_14_71
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.130.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.130.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.130.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_71						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.130.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.131 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_72)

3.131.1 Informationen

ID	TC_Funktion_IFO_14_72
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.131.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.131.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.131.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_72						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.131.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.132 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_73)

3.132.1 Informationen

ID	TC_Funktion_IFO_14_73
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.132.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.132.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.132.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_73						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.132.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.133 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_74)

3.133.1 Informationen

ID	TC_Funktion_IFO_14_74
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.133.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.133.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.133.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_74						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.133.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.134 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_75)

3.134.1 Informationen

ID	TC_Funktion_IFO_14_75
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.134.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.134.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.134.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_75 PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu

verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.134.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.135 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_76)

3.135.1 Informationen

ID	TC_Funktion_IFO_14_76
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.135.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.135.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.135.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_76						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le

00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.135.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.136 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_77)

3.136.1 Informationen

ID	TC_Funktion_IFO_14_77
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.136.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.136.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.136.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_77						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.136.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.137 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_78)

3.137.1 Informationen

ID	TC_Funktion_IFO_14_78
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.137.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.137.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.137.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_78						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.137.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.138 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_79)

3.138.1 Informationen

ID	TC_Funktion_IFO_14_79
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.

Klassifizierung	Fehlerfall-Test

3.138.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.138.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.138.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_79						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.138.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.139 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_80)

3.139.1 Informationen

ID	TC_Funktion_IFO_14_80

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.139.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.139.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.139.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_80						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.139.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.140 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_81)

3.140.1 Informationen

ID	TC_Funktion_IFO_14_81
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.140.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.140.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.140.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_81 ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.140.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.141 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_82)

3.141.1 Informationen

ID	TC_Funktion_IFO_14_82
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.141.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.141.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.141.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_82						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.141.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.142 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_83)

3.142.1 Informationen

ID	TC_Funktion_IFO_14_83
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.142.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.142.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.142.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_83						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le

00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.142.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.143 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_84)

3.143.1 Informationen

ID	TC_Funktion_IFO_14_84
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.143.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.143.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.143.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_84						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.143.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.144 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_85)

3.144.1 Informationen

ID	TC_Funktion_IFO_14_85
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.144.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.144.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.144.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_85						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.144.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.145 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_86)

3.145.1 Informationen

ID	TC_Funktion_IFO_14_86
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.145.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.145.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.145.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_86						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.145.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.146 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_87)

3.146.1 Informationen

ID	TC_Funktion_IFO_14_87
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die

	Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.146.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.146.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.146.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_87 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.146.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.147 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_88)

3.147.1 Informationen

ID	TC_Funktion_IFO_14_88

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.147.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.147.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.147.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_88 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.147.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.148 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_89)

3.148.1 Informationen

ID	TC_Funktion_IFO_14_89
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.148.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.148.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.148.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_89 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve)

86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.148.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.149 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_90)

3.149.1 Informationen

ID	TC_Funktion_IFO_14_90
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.149.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.149.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.149.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_90 GENERAL AUTHENTICATE (ECKA-DH)

CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.149.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.150 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_91)

3.150.1 Informationen

ID	TC_Funktion_IFO_14_91
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.150.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.150.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.150.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_91						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.150.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.151 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_92)

3.151.1 Informationen

ID	TC_Funktion_IFO_14_92
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-

	Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.151.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.151.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.151.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_92						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.151.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.152 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_93)

3.152.1 Informationen

ID	TC_Funktion_IFO_14_93
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.152.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.152.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.152.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_93 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.152.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.153 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_94)

3.153.1 Informationen

ID	TC_Funktion_IFO_14_94
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.153.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.153.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.153.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_94 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.153.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.154 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_95)

3.154.1 Informationen

ID	TC_Funktion_IFO_14_95
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.154.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.154.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.154.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_95						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.154.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.155 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_96)

3.155.1 Informationen

ID	TC_Funktion_IFO_14_96
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.155.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.155.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.155.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_96						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.155.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.156 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_97)

3.156.1 Informationen

ID	TC_Funktion_IFO_14_97
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.156.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.156.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.156.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_97						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.156.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.157 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_98)

3.157.1 Informationen

ID	TC_Funktion_IFO_14_98
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das

	MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.157.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.157.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.157.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_98						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.157.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.158 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_99)

3.158.1 Informationen

ID	TC_Funktion_IFO_14_99
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.158.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.158.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.158.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_99						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu

generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'
Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.158.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.159 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_100)

3.159.1 Informationen

ID	TC_Funktion_IFO_14_100
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.159.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.159.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.159.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_100

GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.159.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.160 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_101)

3.160.1 Informationen

ID	TC_Funktion_IFO_14_101
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.160.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.160.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.160.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_101						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.160.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.161 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_102)

3.161.1 Informationen

ID	TC_Funktion_IFO_14_102
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.161.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.161.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.161.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_102						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.161.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.162 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_103)

3.162.1 Informationen

ID	TC_Funktion_IFO_14_103
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne

	Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.162.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.162.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.162.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_103 PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.162.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.163 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_104)

3.163.1 Informationen

ID	TC_Funktion_IFO_14_104
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien

	und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.163.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.163.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.163.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_104						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.163.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.164 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_105)

3.164.1 Informationen

ID	TC_Funktion_IFO_14_105
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.164.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.164.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.164.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_105						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.164.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.165 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_106)

3.165.1 Informationen

ID	TC_Funktion_IFO_14_106
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.165.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.165.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.165.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_106 PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.165.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.166 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_107)

3.166.1 Informationen

ID	TC_Funktion_IFO_14_107
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.166.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.166.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.166.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_107						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.166.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.167 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_108)

3.167.1 Informationen

ID	TC_Funktion_IFO_14_108
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.167.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.167.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.167.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_108						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.167.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.168 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_109)

3.168.1 Informationen

ID	TC_Funktion_IFO_14_109
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.168.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.168.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.168.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_109						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.168.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.169 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_110)

3.169.1 Informationen

ID	TC_Funktion_IFO_14_110
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-

	Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.169.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.169.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.169.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_110						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.169.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.170 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_111)

3.170.1 Informationen

ID	TC_Funktion_IFO_14_111
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.170.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.170.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.170.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_111 ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.170.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.171 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_112)

3.171.1 Informationen

ID	TC_Funktion_IFO_14_112
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.171.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.171.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.171.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_112 ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.171.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.172 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_113)

3.172.1 Informationen

ID	TC_Funktion_IFO_14_113
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.172.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.172.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.172.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_113
CREATE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.172.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.173 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_114)

3.173.1 Informationen

ID	TC_Funktion_IFO_14_114
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.173.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.173.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.173.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_114						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.173.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.174 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_115)

3.174.1 Informationen

ID	TC_Funktion_IFO_14_115
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.174.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.174.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.174.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_115						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.174.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.175 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_116)

3.175.1 Informationen

ID	TC_Funktion_IFO_14_116
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.175.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.175.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.175.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_116						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.175.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.176 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_117)

3.176.1 Informationen

ID	TC_Funktion_IFO_14_117
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die

	Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.176.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.176.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.176.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_117						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.176.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.177 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_118)

3.177.1 Informationen

ID	TC_Funktion_IFO_14_118
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.177.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.177.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.177.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_118						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.177.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.178 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_119)

3.178.1 Informationen

ID	TC_Funktion_IFO_14_119
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.178.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.178.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.178.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_119 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.178.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.179 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_120)

3.179.1 Informationen

ID	TC_Funktion_IFO_14_120
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.179.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.179.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.179.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_120 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.179.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.180 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_121)

3.180.1 Informationen

ID	TC_Funktion_IFO_14_121
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.180.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.180.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.180.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_121						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.180.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.181 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_122)

3.181.1 Informationen

ID	TC_Funktion_IFO_14_122
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.181.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.181.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.181.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_122						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.181.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.182 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_123)

3.182.1 Informationen

ID	TC_Funktion_IFO_14_123
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.182.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.182.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.182.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_123 GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve

implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.182.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.183 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_124)

3.183.1 Informationen

ID	TC_Funktion_IFO_14_124
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.183.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.183.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.183.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_124

GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.183.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.184 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_125)

3.184.1 Informationen

ID	TC_Funktion_IFO_14_125
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.184.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.184.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.184.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_125						
GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.184.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.185 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_126)

3.185.1 Informationen

ID	TC_Funktion_IFO_14_126
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.185.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.185.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.185.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_126						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.185.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.186 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_127)

3.186.1 Informationen

ID	TC_Funktion_IFO_14_127
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien

	und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.186.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.186.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.186.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_127						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.186.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.187 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_128)

3.187.1 Informationen

ID	TC_Funktion_IFO_14_128
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.187.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.187.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.187.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_128						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template

bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.187.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.188 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_129)

3.188.1 Informationen

ID	TC_Funktion_IFO_14_129
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.188.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.188.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.188.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_129
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.188.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.189 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_130)

3.189.1 Informationen

ID	TC_Funktion_IFO_14_130
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.189.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.189.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.189.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_130						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.189.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.190 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_131)

3.190.1 Informationen

ID	TC_Funktion_IFO_14_131
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die

	Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.190.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.190.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.190.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_131						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.190.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.191 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_132)

3.191.1 Informationen

ID	TC_Funktion_IFO_14_132
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.191.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.191.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.191.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_132						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.191.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.192 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_133)

3.192.1 Informationen

ID	TC_Funktion_IFO_14_133
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.192.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.192.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.192.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_133 INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.192.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.193 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_134)

3.193.1 Informationen

ID	TC_Funktion_IFO_14_134
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.193.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.193.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.193.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_134 PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.193.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.194 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_135)

3.194.1 Informationen

ID	TC_Funktion_IFO_14_135
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.194.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.194.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.194.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_135
PSO COMPUTE DIGITAL SIGNATURE

CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.194.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.195 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_136)

3.195.1 Informationen

ID	TC_Funktion_IFO_14_136
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.195.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.195.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.195.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_136						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.195.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.196 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_137)

3.196.1 Informationen

ID	TC_Funktion_IFO_14_137
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.196.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.196.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.196.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_137						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.196.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.197 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_138)

3.197.1 Informationen

ID	TC_Funktion_IFO_14_138
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien

	und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.197.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.197.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.197.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_138						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.197.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.198 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_139)

3.198.1 Informationen

ID	TC_Funktion_IFO_14_139
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.198.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.198.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.198.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_139						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.198.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.199 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_140)

3.199.1 Informationen

ID	TC_Funktion_IFO_14_140
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.199.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.199.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.199.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_140 PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.199.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.200 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_141)

3.200.1 Informationen

ID	TC_Funktion_IFO_14_141
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.200.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.200.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.200.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_141

PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.200.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.201 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_142)

3.201.1 Informationen

ID	TC_Funktion_IFO_14_142
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.201.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.201.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.201.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_142						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.201.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.202 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_143)

3.202.1 Informationen

ID	TC_Funktion_IFO_14_143
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.202.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.202.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.202.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_143						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.202.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.203 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_144)

3.203.1 Informationen

ID	TC_Funktion_IFO_14_144
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.203.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.203.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.203.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_144						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.203.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.204 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_145)

3.204.1 Informationen

ID	TC_Funktion_IFO_14_145
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das

	Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.204.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.204.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.204.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_145						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.204.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.205 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_146)

3.205.1 Informationen

ID	TC_Funktion_IFO_14_146

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.205.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.205.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.205.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_146						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.205.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.206 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_147)

3.206.1 Informationen

ID	TC_Funktion_IFO_14_147
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.206.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.206.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.206.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_147 DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.206.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.207 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_148)

3.207.1 Informationen

ID	TC_Funktion_IFO_14_148
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.207.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.207.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.207.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_148						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.207.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.208 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_149)

3.208.1 Informationen

ID	TC_Funktion_IFO_14_149
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.208.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.208.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.208.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_149

EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.208.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.209 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_150)

3.209.1 Informationen

ID	TC_Funktion_IFO_14_150
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.209.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.209.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.209.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_150 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.209.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.210 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_151)

3.210.1 Informationen

ID	TC_Funktion_IFO_14_151
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.210.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.210.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.210.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_151						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.210.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.211 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_152)

3.211.1 Informationen

ID	TC_Funktion_IFO_14_152
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.

Klassifizierung	Fehlerfall-Test

3.211.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.211.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.211.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_152						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.211.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.212 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_153)

3.212.1 Informationen

ID	TC_Funktion_IFO_14_153
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.212.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.212.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.212.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_153 GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve

implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.212.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.213 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_154)

3.213.1 Informationen

ID	TC_Funktion_IFO_14_154
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.213.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.213.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.213.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_154

GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.213.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.214 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_155)

3.214.1 Informationen

ID	TC_Funktion_IFO_14_155
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.214.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.214.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.214.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_155						
GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.214.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.215 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_156)

3.215.1 Informationen

ID	TC_Funktion_IFO_14_156
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-

	Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.215.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.215.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.215.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_156 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.215.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.216 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_157)

3.216.1 Informationen

ID	TC_Funktion_IFO_14_157
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.216.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.216.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.216.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_157 GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.216.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.217 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_158)

3.217.1 Informationen

ID	TC_Funktion_IFO_14_158
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.217.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.217.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.217.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_158						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.217.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.218 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_159)

3.218.1 Informationen

ID	TC_Funktion_IFO_14_159
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.218.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.218.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.218.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_159

GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.218.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.219 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_160)

3.219.1 Informationen

ID	TC_Funktion_IFO_14_160
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.219.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.219.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.219.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_160						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.219.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.220 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_161)

3.220.1 Informationen

ID	TC_Funktion_IFO_14_161
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne

	Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.220.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.220.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.220.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_161						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.220.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.221 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_162)

3.221.1 Informationen

ID	TC_Funktion_IFO_14_162
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.221.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.221.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.221.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_162						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu

generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'
Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.221.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.222 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_163)

3.222.1 Informationen

ID	TC_Funktion_IFO_14_163
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.222.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.222.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.222.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_163 INTERNAL AUTHENTICATE

CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.222.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.223 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_164)

3.223.1 Informationen

ID	TC_Funktion_IFO_14_164
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.223.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.223.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.223.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_164						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.223.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.224 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_165)

3.224.1 Informationen

ID	TC_Funktion_IFO_14_165
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.224.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.224.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.224.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_165 PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.224.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.225 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_166)

3.225.1 Informationen

ID	TC_Funktion_IFO_14_166
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.225.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.225.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.225.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_166						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.225.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.226 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_167)

3.226.1 Informationen

ID	TC_Funktion_IFO_14_167
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.226.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.226.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.226.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_167 PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.226.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.227 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_168)

3.227.1 Informationen

ID	TC_Funktion_IFO_14_168
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.227.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.227.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.227.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_168						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu

verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.227.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.228 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_169)

3.228.1 Informationen

ID	TC_Funktion_IFO_14_169
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.228.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.228.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.228.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_169						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le

00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.228.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.229 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_170)

3.229.1 Informationen

ID	TC_Funktion_IFO_14_170
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.229.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.229.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.229.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_170						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.229.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.230 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_171)

3.230.1 Informationen

ID	TC_Funktion_IFO_14_171
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.230.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.230.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.230.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_171						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.230.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.231 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_172)

3.231.1 Informationen

ID	TC_Funktion_IFO_14_172
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.

Klassifizierung	Fehlerfall-Test

3.231.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.231.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.231.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_172						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.231.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.232 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_173)

3.232.1 Informationen

ID	TC_Funktion_IFO_14_173

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.232.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.232.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.232.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_173						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.232.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.233 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_174)

3.233.1 Informationen

ID	TC_Funktion_IFO_14_174
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.233.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.233.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.233.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_174 ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.233.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.234 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_175)

3.234.1 Informationen

ID	TC_Funktion_IFO_14_175
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.234.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.234.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.234.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_175						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.234.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.235 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_176)

3.235.1 Informationen

ID	TC_Funktion_IFO_14_176
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.235.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.235.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.235.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_176						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le

00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.235.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.236 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_177)

3.236.1 Informationen

ID	TC_Funktion_IFO_14_177
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.236.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.236.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.236.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_177						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.236.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.237 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_178)

3.237.1 Informationen

ID	TC_Funktion_IFO_14_178
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.237.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.237.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.237.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_178						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.237.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.238 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_179)

3.238.1 Informationen

ID	TC_Funktion_IFO_14_179
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.238.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.238.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.238.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_179						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.238.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.239 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_180)

3.239.1 Informationen

ID	TC_Funktion_IFO_14_180
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die

	Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.239.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.239.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.239.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_180 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.239.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.240 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_181)

3.240.1 Informationen

ID	TC_Funktion_IFO_14_181

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.240.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.240.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.240.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_181 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.240.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.241 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_182)

3.241.1 Informationen

ID	TC_Funktion_IFO_14_182
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.241.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.241.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.241.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_182 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve)

86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.241.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.242 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_183)

3.242.1 Informationen

ID	TC_Funktion_IFO_14_183
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.242.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.242.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.242.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_183
GENERAL AUTHENTICATE (ECKA-DH)

CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.242.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.243 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_184)

3.243.1 Informationen

ID	TC_Funktion_IFO_14_184
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.243.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.243.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.243.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_184						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.243.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.244 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_185)

3.244.1 Informationen

ID	TC_Funktion_IFO_14_185
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-

	Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.244.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.244.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.244.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_185 GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.244.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.245 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_186)

3.245.1 Informationen

ID	TC_Funktion_IFO_14_186
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.245.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.245.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.245.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_186 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.245.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.246 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_187)

3.246.1 Informationen

ID	TC_Funktion_IFO_14_187
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.246.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.246.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.246.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_187 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.246.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.247 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_188)

3.247.1 Informationen

ID	TC_Funktion_IFO_14_188
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.247.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.247.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.247.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_188						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.247.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.248 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_189)

3.248.1 Informationen

ID	TC_Funktion_IFO_14_189
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.248.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.248.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.248.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_189						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.248.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.249 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_190)

3.249.1 Informationen

ID	TC_Funktion_IFO_14_190
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.249.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.249.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.249.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_190						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.249.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.250 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_191)

3.250.1 Informationen

ID	TC_Funktion_IFO_14_191
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das

	MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.250.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.250.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.250.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_191						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.250.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.251 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_192)

3.251.1 Informationen

ID	TC_Funktion_IFO_14_192
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.251.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.251.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.251.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_192						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu

generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'
Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.251.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.252 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_193)

3.252.1 Informationen

ID	TC_Funktion_IFO_14_193
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.252.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.252.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.252.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_193

GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.252.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.253 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_194)

3.253.1 Informationen

ID	TC_Funktion_IFO_14_194
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.253.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.253.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.253.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_194 INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.253.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.254 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_195)

3.254.1 Informationen

ID	TC_Funktion_IFO_14_195
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.254.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.254.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.254.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_195						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.254.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.255 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_196)

3.255.1 Informationen

ID	TC_Funktion_IFO_14_196
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne

	Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.255.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.255.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.255.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_196 PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.255.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.256 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_197)

3.256.1 Informationen

ID	TC_Funktion_IFO_14_197
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien

	und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.256.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.256.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.256.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_197						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.256.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.257 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_198)

3.257.1 Informationen

ID	TC_Funktion_IFO_14_198
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.257.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.257.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.257.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_198						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.257.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.258 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_199)

3.258.1 Informationen

ID	TC_Funktion_IFO_14_199
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.258.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.258.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.258.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_199 PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.258.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.259 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_200)

3.259.1 Informationen

ID	TC_Funktion_IFO_14_200
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.259.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.259.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.259.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_200						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.259.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.260 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_201)

3.260.1 Informationen

ID	TC_Funktion_IFO_14_201
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.260.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.260.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.260.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_201						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.260.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.261 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_202)

3.261.1 Informationen

ID	TC_Funktion_IFO_14_202
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.261.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.261.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.261.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_202						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.261.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.262 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_203)

3.262.1 Informationen

ID	TC_Funktion_IFO_14_203
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-

	Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_TLS_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.262.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.262.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.262.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_203						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.262.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.263 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_204)

3.263.1 Informationen

ID	TC_Funktion_IFO_14_204
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.263.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.263.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.263.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_204						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.263.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.264 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_205)

3.264.1 Informationen

ID	TC_Funktion_IFO_14_205
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.264.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.264.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.264.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_205						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.264.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.265 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_206)

3.265.1 Informationen

ID	TC_Funktion_IFO_14_206
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.265.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.265.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.265.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_206
CREATE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.265.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.266 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_207)

3.266.1 Informationen

ID	TC_Funktion_IFO_14_207
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.266.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.266.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.266.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_207						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.266.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.267 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_208)

3.267.1 Informationen

ID	TC_Funktion_IFO_14_208
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.267.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.267.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.267.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_208						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.267.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.268 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_209)

3.268.1 Informationen

ID	TC_Funktion_IFO_14_209
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.268.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.268.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.268.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_209						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.268.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.269 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_210)

3.269.1 Informationen

ID	TC_Funktion_IFO_14_210
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die

	Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.269.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.269.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.269.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_210						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.269.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.270 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_211)

3.270.1 Informationen

ID	TC_Funktion_IFO_14_211
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.270.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.270.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.270.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_211						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.270.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.271 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_212)

3.271.1 Informationen

ID	TC_Funktion_IFO_14_212
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.271.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.271.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.271.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_212 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.271.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.272 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_213)

3.272.1 Informationen

ID	TC_Funktion_IFO_14_213
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.272.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.272.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.272.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_213 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.272.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.273 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_214)

3.273.1 Informationen

ID	TC_Funktion_IFO_14_214
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.273.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.273.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.273.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_214						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.273.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.274 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_215)

3.274.1 Informationen

ID	TC_Funktion_IFO_14_215
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.274.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.274.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.274.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_215						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.274.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.275 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_216)

3.275.1 Informationen

ID	TC_Funktion_IFO_14_216
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.275.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.275.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.275.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_216 GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve

implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.275.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.276 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_217)

3.276.1 Informationen

ID	TC_Funktion_IFO_14_217
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.276.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.276.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.276.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_217

GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.276.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.277 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_218)

3.277.1 Informationen

ID	TC_Funktion_IFO_14_218
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.277.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.277.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.277.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_218						
GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.277.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.278 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_219)

3.278.1 Informationen

ID	TC_Funktion_IFO_14_219
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.278.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.278.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.278.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_219						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.278.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.279 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_220)

3.279.1 Informationen

ID	TC_Funktion_IFO_14_220
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien

	und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.279.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.279.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.279.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_220						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.279.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.280 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_221)

3.280.1 Informationen

ID	TC_Funktion_IFO_14_221
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.280.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.280.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.280.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_221						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template

bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.280.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.281 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_222)

3.281.1 Informationen

ID	TC_Funktion_IFO_14_222
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.281.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.281.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.281.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_222
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.281.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.282 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_223)

3.282.1 Informationen

ID	TC_Funktion_IFO_14_223
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.282.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.282.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.282.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_223						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.282.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.283 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_224)

3.283.1 Informationen

ID	TC_Funktion_IFO_14_224
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die

	Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.283.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.283.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.283.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_224						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.283.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.284 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_225)

3.284.1 Informationen

ID	TC_Funktion_IFO_14_225
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.284.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.284.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.284.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_225						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.284.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.285 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_226)

3.285.1 Informationen

ID	TC_Funktion_IFO_14_226
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.285.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.285.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.285.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_226 INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.285.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.286 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_227)

3.286.1 Informationen

ID	TC_Funktion_IFO_14_227
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.286.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.286.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.286.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_227 PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.286.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.287 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_228)

3.287.1 Informationen

ID	TC_Funktion_IFO_14_228
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.287.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.287.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.287.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_228 PSO COMPUTE DIGITAL SIGNATURE

CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.287.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.288 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_229)

3.288.1 Informationen

ID	TC_Funktion_IFO_14_229
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.288.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.288.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.288.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_229						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.288.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.289 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_230)

3.289.1 Informationen

ID	TC_Funktion_IFO_14_230
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.289.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.289.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.289.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_230						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.289.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.290 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_231)

3.290.1 Informationen

ID	TC_Funktion_IFO_14_231
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien

	und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.290.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.290.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.290.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_231						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.290.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.291 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_232)

3.291.1 Informationen

ID	TC_Funktion_IFO_14_232
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.291.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.291.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.291.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_232						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.291.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.292 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_233)

3.292.1 Informationen

ID	TC_Funktion_IFO_14_233
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.292.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.292.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.292.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_233						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.292.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.293 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_234)

3.293.1 Informationen

ID	TC_Funktion_IFO_14_234
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_SIG_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.293.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.293.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.293.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_234

PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.293.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.294 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_235)

3.294.1 Informationen

ID	TC_Funktion_IFO_14_235
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.294.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.294.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.294.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_235						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.294.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.295 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_236)

3.295.1 Informationen

ID	TC_Funktion_IFO_14_236
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.295.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.295.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.295.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_236						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.295.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.296 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_237)

3.296.1 Informationen

ID	TC_Funktion_IFO_14_237
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.296.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.296.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.296.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_237						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.296.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.297 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_238)

3.297.1 Informationen

ID	TC_Funktion_IFO_14_238
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das

	Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.297.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.297.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.297.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_238						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.297.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.298 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_239)

3.298.1 Informationen

ID	TC_Funktion_IFO_14_239

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.298.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.298.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.298.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_239						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.298.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.299 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_240)

3.299.1 Informationen

ID	TC_Funktion_IFO_14_240
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.299.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.299.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.299.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_240						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.299.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.300 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_241)

3.300.1 Informationen

ID	TC_Funktion_IFO_14_241
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.300.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.300.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.300.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_241 DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.300.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.301 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_242)

3.301.1 Informationen

ID	TC_Funktion_IFO_14_242
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.301.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.301.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.301.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_242

EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.301.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.302 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_243)

3.302.1 Informationen

ID	TC_Funktion_IFO_14_243
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.302.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.302.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.302.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_243						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.302.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.303 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_244)

3.303.1 Informationen

ID	TC_Funktion_IFO_14_244
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.303.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.303.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.303.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_244						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.303.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.304 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_245)

3.304.1 Informationen

ID	TC_Funktion_IFO_14_245
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.

Klassifizierung	Fehlerfall-Test

3.304.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.304.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.304.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_245 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.304.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.305 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_246)

3.305.1 Informationen

ID	TC_Funktion_IFO_14_246
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.305.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.305.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.305.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_246 GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve

implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.305.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.306 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_247)

3.306.1 Informationen

ID	TC_Funktion_IFO_14_247
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.306.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.306.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.306.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_247

GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.306.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.307 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_248)

3.307.1 Informationen

ID	TC_Funktion_IFO_14_248
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.307.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.307.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.307.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_248						
GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.307.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.308 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_249)

3.308.1 Informationen

ID	TC_Funktion_IFO_14_249
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-

	Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.308.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.308.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.308.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_249 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.308.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.309 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_250)

3.309.1 Informationen

ID	TC_Funktion_IFO_14_250
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.309.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.309.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.309.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_250						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.309.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.310 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_251)

3.310.1 Informationen

ID	TC_Funktion_IFO_14_251
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.310.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.310.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.310.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_251 GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.310.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.311 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_252)

3.311.1 Informationen

ID	TC_Funktion_IFO_14_252
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.311.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.311.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.311.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_252

GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.311.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.312 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_253)

3.312.1 Informationen

ID	TC_Funktion_IFO_14_253
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.312.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.312.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.312.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_253						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.312.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.313 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_254)

3.313.1 Informationen

ID	TC_Funktion_IFO_14_254
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne

	Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.313.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.313.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.313.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_254						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.313.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.314 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_255)

3.314.1 Informationen

ID	TC_Funktion_IFO_14_255
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.314.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.314.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.314.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_255						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu

generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'
Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.314.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.315 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_256)

3.315.1 Informationen

ID	TC_Funktion_IFO_14_256
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.315.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.315.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.315.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_256
INTERNAL AUTHENTICATE

CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.315.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.316 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_257)

3.316.1 Informationen

ID	TC_Funktion_IFO_14_257
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.316.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.316.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.316.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_257						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.316.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.317 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_258)

3.317.1 Informationen

ID	TC_Funktion_IFO_14_258
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.317.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.317.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.317.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_258 PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.317.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.318 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_259)

3.318.1 Informationen

ID	TC_Funktion_IFO_14_259
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.318.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.318.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.318.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_259						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.318.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.319 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_260)

3.319.1 Informationen

ID	TC_Funktion_IFO_14_260
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.319.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.319.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.319.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_260						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.319.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.320 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_261)

3.320.1 Informationen

ID	TC_Funktion_IFO_14_261
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.320.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.320.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.320.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_261						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu

verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.320.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.321 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_262)

3.321.1 Informationen

ID	TC_Funktion_IFO_14_262
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.321.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.321.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.321.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_262						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le

00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.321.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.322 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_263)

3.322.1 Informationen

ID	TC_Funktion_IFO_14_263
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.322.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.322.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.322.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_263						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.322.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.323 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_264)

3.323.1 Informationen

ID	TC_Funktion_IFO_14_264
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.323.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.323.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.323.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_264						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.323.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.324 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_265)

3.324.1 Informationen

ID	TC_Funktion_IFO_14_265
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_ENC_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.

Klassifizierung	Fehlerfall-Test

3.324.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.324.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.324.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_265						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.324.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.325 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_266)

3.325.1 Informationen

ID	TC_Funktion_IFO_14_266

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.325.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.325.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.325.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_266						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.325.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.326 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_267)

3.326.1 Informationen

ID	TC_Funktion_IFO_14_267
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.326.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.326.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.326.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_267						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.326.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.327 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_268)

3.327.1 Informationen

ID	TC_Funktion_IFO_14_268
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.327.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.327.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.327.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_268						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.327.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.328 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_269)

3.328.1 Informationen

ID	TC_Funktion_IFO_14_269
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.328.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.328.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.328.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_269						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le

00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.328.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.329 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_270)

3.329.1 Informationen

ID	TC_Funktion_IFO_14_270
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.329.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.329.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.329.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_270						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.329.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.330 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_271)

3.330.1 Informationen

ID	TC_Funktion_IFO_14_271
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.330.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.330.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.330.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_271						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.330.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.331 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_272)

3.331.1 Informationen

ID	TC_Funktion_IFO_14_272
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.331.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.331.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.331.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_272						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.331.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.332 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_273)

3.332.1 Informationen

ID	TC_Funktion_IFO_14_273
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die

	Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.332.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.332.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.332.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_273						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.332.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.333 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_274)

3.333.1 Informationen

ID	TC_Funktion_IFO_14_274

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.333.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.333.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.333.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_274						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.333.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.334 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_275)

3.334.1 Informationen

ID	TC_Funktion_IFO_14_275
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.334.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.334.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.334.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_275 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve)

86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.334.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.335 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_276)

3.335.1 Informationen

ID	TC_Funktion_IFO_14_276
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.335.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.335.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.335.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_276 GENERAL AUTHENTICATE (ECKA-DH)

CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.335.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.336 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_277)

3.336.1 Informationen

ID	TC_Funktion_IFO_14_277
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.336.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.336.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.336.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_277						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.336.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.337 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_278)

3.337.1 Informationen

ID	TC_Funktion_IFO_14_278
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-

	Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.337.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.337.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.337.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_278 GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.337.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.338 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_279)

3.338.1 Informationen

ID	TC_Funktion_IFO_14_279
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.338.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.338.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.338.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_279 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.338.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.339 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_280)

3.339.1 Informationen

ID	TC_Funktion_IFO_14_280
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.339.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.339.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.339.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_280 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.339.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.340 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_281)

3.340.1 Informationen

ID	TC_Funktion_IFO_14_281
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.340.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.340.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.340.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_281						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.340.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.341 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_282)

3.341.1 Informationen

ID	TC_Funktion_IFO_14_282
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.341.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.341.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.341.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_282						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.341.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.342 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_283)

3.342.1 Informationen

ID	TC_Funktion_IFO_14_283
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.342.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.342.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.342.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_283						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.342.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.343 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_284)

3.343.1 Informationen

ID	TC_Funktion_IFO_14_284
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das

	MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.343.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.343.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.343.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_284						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.343.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.344 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_285)

3.344.1 Informationen

ID	TC_Funktion_IFO_14_285
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.344.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.344.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.344.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_285						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu

generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'
Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.344.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.345 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_286)

3.345.1 Informationen

ID	TC_Funktion_IFO_14_286
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.345.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.345.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.345.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_286

GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.345.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.346 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_287)

3.346.1 Informationen

ID	TC_Funktion_IFO_14_287
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.346.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.346.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.346.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_287						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.346.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.347 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_288)

3.347.1 Informationen

ID	TC_Funktion_IFO_14_288
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.347.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.347.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.347.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_288						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.347.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.348 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_289)

3.348.1 Informationen

ID	TC_Funktion_IFO_14_289
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne

	Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.348.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.348.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.348.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_289 PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.348.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.349 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_290)

3.349.1 Informationen

ID	TC_Funktion_IFO_14_290
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien

	und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.349.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.349.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.349.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_290						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.349.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.350 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_291)

3.350.1 Informationen

ID	TC_Funktion_IFO_14_291
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.350.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.350.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.350.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_291						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.350.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.351 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_292)

3.351.1 Informationen

ID	TC_Funktion_IFO_14_292
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.351.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.351.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.351.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_292 PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.351.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.352 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_293)

3.352.1 Informationen

ID	TC_Funktion_IFO_14_293
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.352.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.352.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.352.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_293						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.352.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.353 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_294)

3.353.1 Informationen

ID	TC_Funktion_IFO_14_294
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.353.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.353.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.353.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_294						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.353.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.354 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_295)

3.354.1 Informationen

ID	TC_Funktion_IFO_14_295
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.354.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.354.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.354.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_295						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.354.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.355 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_296)

3.355.1 Informationen

ID	TC_Funktion_IFO_14_296
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-

	Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.GWA_AUT_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.355.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.355.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.355.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_296						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.355.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.356 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_297)

3.356.1 Informationen

ID	TC_Funktion_IFO_14_297
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.356.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.356.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.356.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_297						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.356.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.357 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_298)

3.357.1 Informationen

ID	TC_Funktion_IFO_14_298
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.357.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.357.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.357.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_298						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.357.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.358 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_299)

3.358.1 Informationen

ID	TC_Funktion_IFO_14_299
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.358.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.358.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.358.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_299
CREATE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.358.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.359 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_300)

3.359.1 Informationen

ID	TC_Funktion_IFO_14_300
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.359.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.359.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.359.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_300						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.359.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.360 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_301)

3.360.1 Informationen

ID	TC_Funktion_IFO_14_301
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.360.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.360.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.360.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_301						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.360.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.361 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_302)

3.361.1 Informationen

ID	TC_Funktion_IFO_14_302
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.361.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.361.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.361.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_302						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.361.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.362 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_303)

3.362.1 Informationen

ID	TC_Funktion_IFO_14_303
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die

	Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.362.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.362.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.362.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_303						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.362.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.363 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_304)

3.363.1 Informationen

ID	TC_Funktion_IFO_14_304
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.363.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.363.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.363.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_304						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.363.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.364 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_305)

3.364.1 Informationen

ID	TC_Funktion_IFO_14_305
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.364.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.364.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.364.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_305 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.364.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.365 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_306)

3.365.1 Informationen

ID	TC_Funktion_IFO_14_306
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.365.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.365.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.365.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_306 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.365.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.366 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_307)

3.366.1 Informationen

ID	TC_Funktion_IFO_14_307
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.366.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.366.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.366.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_307						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.366.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.367 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_308)

3.367.1 Informationen

ID	TC_Funktion_IFO_14_308
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.367.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.367.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.367.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_308						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.367.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.368 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_309)

3.368.1 Informationen

ID	TC_Funktion_IFO_14_309
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.368.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.368.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.368.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_309 GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve

implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.368.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.369 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_310)

3.369.1 Informationen

ID	TC_Funktion_IFO_14_310
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.369.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.369.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.369.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_310

GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.369.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.370 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_311)

3.370.1 Informationen

ID	TC_Funktion_IFO_14_311
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.370.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.370.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.370.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_311						
GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.370.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.371 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_312)

3.371.1 Informationen

ID	TC_Funktion_IFO_14_312
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.371.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.371.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.371.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_312						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.371.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.372 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_313)

3.372.1 Informationen

ID	TC_Funktion_IFO_14_313
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien

	und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.372.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.372.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.372.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_313						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.372.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.373 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_314)

3.373.1 Informationen

ID	TC_Funktion_IFO_14_314
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.373.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.373.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.373.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_314						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template

bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.373.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.374 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_315)

3.374.1 Informationen

ID	TC_Funktion_IFO_14_315
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.374.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.374.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.374.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_315
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.374.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.375 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_316)

3.375.1 Informationen

ID	TC_Funktion_IFO_14_316
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.375.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.375.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.375.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_316						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.375.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.376 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_317)

3.376.1 Informationen

ID	TC_Funktion_IFO_14_317
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die

	Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.376.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.376.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.376.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_317 GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.376.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.377 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_318)

3.377.1 Informationen

ID	TC_Funktion_IFO_14_318
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.377.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.377.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.377.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_318						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.377.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.378 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_319)

3.378.1 Informationen

ID	TC_Funktion_IFO_14_319
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.378.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.378.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.378.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_319 INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.378.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.379 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_320)

3.379.1 Informationen

ID	TC_Funktion_IFO_14_320
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.379.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.379.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.379.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_320 PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le

00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.379.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.380 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_321)

3.380.1 Informationen

ID	TC_Funktion_IFO_14_321
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.380.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.380.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.380.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_321

PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.380.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.381 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_322)

3.381.1 Informationen

ID	TC_Funktion_IFO_14_322
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.381.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.381.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.381.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_322						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.381.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.382 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_323)

3.382.1 Informationen

ID	TC_Funktion_IFO_14_323
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des

	Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.382.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.382.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.382.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_323						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.382.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.383 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_324)

3.383.1 Informationen

ID	TC_Funktion_IFO_14_324

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.383.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.383.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.383.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_324						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.383.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.384 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_325)

3.384.1 Informationen

ID	TC_Funktion_IFO_14_325
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.384.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.384.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.384.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_325						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.384.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.385 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_326)

3.385.1 Informationen

ID	TC_Funktion_IFO_14_326
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_TRANS, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.385.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.385.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.385.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_326 PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.385.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.386 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_327)

3.386.1 Informationen

ID	TC_Funktion_IFO_14_327
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.386.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.386.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.386.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_327

ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.386.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.387 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_328)

3.387.1 Informationen

ID	TC_Funktion_IFO_14_328
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.387.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.387.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.387.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_328						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.387.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.388 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_329)

3.388.1 Informationen

ID	TC_Funktion_IFO_14_329
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.388.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.388.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.388.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_329						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.388.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.389 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_330)

3.389.1 Informationen

ID	TC_Funktion_IFO_14_330
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.389.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.389.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.389.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_330						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.389.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.390 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_331)

3.390.1 Informationen

ID	TC_Funktion_IFO_14_331
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das

	Kommando 'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.390.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.390.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.390.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_331						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.390.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.391 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_332)

3.391.1 Informationen

ID	TC_Funktion_IFO_14_332

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.391.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.391.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.391.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_332						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.391.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.392 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_333)

3.392.1 Informationen

ID	TC_Funktion_IFO_14_333
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.392.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.392.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.392.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_333						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.392.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.393 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_334)

3.393.1 Informationen

ID	TC_Funktion_IFO_14_334
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.393.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.393.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.393.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_334 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.393.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.394 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_335)

3.394.1 Informationen

ID	TC_Funktion_IFO_14_335
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.394.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.394.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.394.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_335						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le

00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.394.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.395 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_336)

3.395.1 Informationen

ID	TC_Funktion_IFO_14_336
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.395.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.395.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.395.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_336

GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.395.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.396 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_337)

3.396.1 Informationen

ID	TC_Funktion_IFO_14_337
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.396.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.396.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.396.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_337						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.396.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.397 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_338)

3.397.1 Informationen

ID	TC_Funktion_IFO_14_338
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die

	Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.397.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.397.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.397.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_338 GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.397.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.398 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_339)

3.398.1 Informationen

ID	TC_Funktion_IFO_14_339
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.398.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.398.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.398.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_339 GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve

implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.398.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.399 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_340)

3.399.1 Informationen

ID	TC_Funktion_IFO_14_340
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.399.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.399.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.399.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_340

GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.399.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.400 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_341)

3.400.1 Informationen

ID	TC_Funktion_IFO_14_341
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.400.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.400.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.400.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_341						
GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.400.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.401 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_342)

3.401.1 Informationen

ID	TC_Funktion_IFO_14_342
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.401.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.401.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.401.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_342						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.401.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.402 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_343)

3.402.1 Informationen

ID	TC_Funktion_IFO_14_343
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien

	und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.402.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.402.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.402.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_343						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.402.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.403 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_344)

3.403.1 Informationen

ID	TC_Funktion_IFO_14_344
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.403.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.403.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.403.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_344						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template

bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.403.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.404 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_345)

3.404.1 Informationen

ID	TC_Funktion_IFO_14_345
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.404.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.404.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.404.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_345
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.404.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.405 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_346)

3.405.1 Informationen

ID	TC_Funktion_IFO_14_346
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.405.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.405.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.405.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_346						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.405.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.406 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_347)

3.406.1 Informationen

ID	TC_Funktion_IFO_14_347
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die

	Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.406.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.406.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.406.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_347						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.406.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.407 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_348)

3.407.1 Informationen

ID	TC_Funktion_IFO_14_348
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.407.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.407.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.407.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_348						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.407.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.408 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_349)

3.408.1 Informationen

ID	TC_Funktion_IFO_14_349
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.408.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.408.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.408.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_349						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.408.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.409 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_350)

3.409.1 Informationen

ID	TC_Funktion_IFO_14_350
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.409.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.409.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.409.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_350						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le

00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.409.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.410 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_351)

3.410.1 Informationen

ID	TC_Funktion_IFO_14_351
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.410.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.410.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.410.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_351						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.410.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.411 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_352)

3.411.1 Informationen

ID	TC_Funktion_IFO_14_352
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.411.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.411.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.411.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_352						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.411.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.412 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_353)

3.412.1 Informationen

ID	TC_Funktion_IFO_14_353
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das

	Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.412.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.412.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.412.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_353						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.412.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.413 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_354)

3.413.1 Informationen

ID	TC_Funktion_IFO_14_354

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.413.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.413.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.413.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_354						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.413.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.414 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_355)

3.414.1 Informationen

ID	TC_Funktion_IFO_14_355
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP_PUB_TRANS, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.414.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.414.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.414.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_355						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.414.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.415 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_356)

3.415.1 Informationen

ID	TC_Funktion_IFO_14_356
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.415.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.415.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.415.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_356						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.415.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.416 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_357)

3.416.1 Informationen

ID	TC_Funktion_IFO_14_357
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.416.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.416.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.416.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_357
ACTIVATE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.416.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.417 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_358)

3.417.1 Informationen

ID	TC_Funktion_IFO_14_358
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.417.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.417.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.417.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_358						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.417.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.418 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_359)

3.418.1 Informationen

ID	TC_Funktion_IFO_14_359
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.418.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.418.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.418.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_359						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.418.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.419 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_360)

3.419.1 Informationen

ID	TC_Funktion_IFO_14_360
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.419.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.419.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.419.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_360						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.419.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.420 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_361)

3.420.1 Informationen

ID	TC_Funktion_IFO_14_361
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die

	Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.420.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.420.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.420.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_361						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.420.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.421 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_362)

3.421.1 Informationen

ID	TC_Funktion_IFO_14_362
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.421.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.421.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.421.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_362						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.421.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.422 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_363)

3.422.1 Informationen

ID	TC_Funktion_IFO_14_363
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.422.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.422.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.422.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_363 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.422.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.423 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_364)

3.423.1 Informationen

ID	TC_Funktion_IFO_14_364
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.423.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.423.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.423.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_364 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.423.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.424 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_365)

3.424.1 Informationen

ID	TC_Funktion_IFO_14_365
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.424.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.424.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.424.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_365						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.424.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.425 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_366)

3.425.1 Informationen

ID	TC_Funktion_IFO_14_366
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.425.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.425.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.425.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_366						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.425.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.426 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_367)

3.426.1 Informationen

ID	TC_Funktion_IFO_14_367
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.426.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.426.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.426.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_367 GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve

implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.426.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.427 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_368)

3.427.1 Informationen

ID	TC_Funktion_IFO_14_368
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.427.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.427.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.427.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_368 GENERAL AUTHENTICATE (PACE)

CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.427.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.428 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_369)

3.428.1 Informationen

ID	TC_Funktion_IFO_14_369
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.428.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.428.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.428.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_369						
GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.428.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.429 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_370)

3.429.1 Informationen

ID	TC_Funktion_IFO_14_370
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.429.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.429.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.429.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_370						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.429.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.430 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_371)

3.430.1 Informationen

ID	TC_Funktion_IFO_14_371
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando

	'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.430.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.430.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.430.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_371						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.430.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.431 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_372)

3.431.1 Informationen

ID	TC_Funktion_IFO_14_372
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.431.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.431.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.431.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_372						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template

bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.431.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.432 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_373)

3.432.1 Informationen

ID	TC_Funktion_IFO_14_373
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.432.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.432.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.432.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_373 INTERNAL AUTHENTICATE

CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.432.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.433 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_374)

3.433.1 Informationen

ID	TC_Funktion_IFO_14_374
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.433.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.433.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.433.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_374						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.433.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.434 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_375)

3.434.1 Informationen

ID	TC_Funktion_IFO_14_375
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.434.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.434.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.434.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_375 PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.434.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.435 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_376)

3.435.1 Informationen

ID	TC_Funktion_IFO_14_376
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.435.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.435.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.435.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_376						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.435.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.436 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_377)

3.436.1 Informationen

ID	TC_Funktion_IFO_14_377
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien

	und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.436.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.436.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.436.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_377						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.436.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.437 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_378)

3.437.1 Informationen

ID	TC_Funktion_IFO_14_378
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.437.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.437.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.437.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_378						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.437.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.438 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_379)

3.438.1 Informationen

ID	TC_Funktion_IFO_14_379
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.438.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.438.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.438.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_379						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.438.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.439 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_380)

3.439.1 Informationen

ID	TC_Funktion_IFO_14_380
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.439.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.439.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.439.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_380
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.439.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.440 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_381)

3.440.1 Informationen

ID	TC_Funktion_IFO_14_381
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.IMP, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.440.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.440.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.440.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_381 PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.440.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.441 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_382)

3.441.1 Informationen

ID	TC_Funktion_IFO_14_382
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.441.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.441.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.441.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_382						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.441.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.442 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_383)

3.442.1 Informationen

ID	TC_Funktion_IFO_14_383
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die

	Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.442.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.442.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.442.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_383						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.442.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.443 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_384)

3.443.1 Informationen

ID	TC_Funktion_IFO_14_384
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.443.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.443.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.443.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_384 CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.443.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.444 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_385)

3.444.1 Informationen

ID	TC_Funktion_IFO_14_385
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.444.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.444.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.444.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_385						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.444.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.445 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_386)

3.445.1 Informationen

ID	TC_Funktion_IFO_14_386
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.445.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.445.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.445.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_386

DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.445.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.446 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_387)

3.446.1 Informationen

ID	TC_Funktion_IFO_14_387
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.446.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.446.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.446.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_387						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.446.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.447 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_388)

3.447.1 Informationen

ID	TC_Funktion_IFO_14_388
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.447.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.447.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.447.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_388						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.447.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.448 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_389)

3.448.1 Informationen

ID	TC_Funktion_IFO_14_389
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.

Klassifizierung	Fehlerfall-Test

3.448.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.448.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.448.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_389 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.448.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.449 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_390)

3.449.1 Informationen

ID	TC_Funktion_IFO_14_390
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die

	Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.449.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.449.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.449.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_390 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.449.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.450 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_391)

3.450.1 Informationen

ID	TC_Funktion_IFO_14_391
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.450.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.450.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.450.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_391 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve)

86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.450.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.451 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_392)

3.451.1 Informationen

ID	TC_Funktion_IFO_14_392
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.451.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.451.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.451.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_392 GENERAL AUTHENTICATE (ECKA-EG)

CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.451.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.452 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_393)

3.452.1 Informationen

ID	TC_Funktion_IFO_14_393
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.452.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.452.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.452.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_393						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.452.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.453 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_394)

3.453.1 Informationen

ID	TC_Funktion_IFO_14_394
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-

	Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.453.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.453.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.453.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_394 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.453.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.454 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_395)

3.454.1 Informationen

ID	TC_Funktion_IFO_14_395
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.454.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.454.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.454.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_395 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.454.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.455 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_396)

3.455.1 Informationen

ID	TC_Funktion_IFO_14_396
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.455.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.455.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.455.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_396						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.455.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.456 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_397)

3.456.1 Informationen

ID	TC_Funktion_IFO_14_397
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.456.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.456.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.456.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_397
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.456.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.457 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_398)

3.457.1 Informationen

ID	TC_Funktion_IFO_14_398
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.457.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.457.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.457.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_398						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.457.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.458 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_399)

3.458.1 Informationen

ID	TC_Funktion_IFO_14_399
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.458.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.458.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.458.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_399						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.458.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.459 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_400)

3.459.1 Informationen

ID	TC_Funktion_IFO_14_400
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das

	MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.459.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.459.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.459.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_400						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.459.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.460 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_401)

3.460.1 Informationen

ID	TC_Funktion_IFO_14_401
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.460.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.460.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.460.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_401 GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu

generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'
Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.460.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.461 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_402)

3.461.1 Informationen

ID	TC_Funktion_IFO_14_402
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.461.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.461.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.461.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_402 INTERNAL AUTHENTICATE

CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.461.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.462 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_403)

3.462.1 Informationen

ID	TC_Funktion_IFO_14_403
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.462.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.462.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.462.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_403						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.462.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.463 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_404)

3.463.1 Informationen

ID	TC_Funktion_IFO_14_404
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.463.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.463.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.463.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_404 PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.463.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.464 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_405)

3.464.1 Informationen

ID	TC_Funktion_IFO_14_405
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.464.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.464.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.464.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_405						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.464.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.465 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_406)

3.465.1 Informationen

ID	TC_Funktion_IFO_14_406
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand

	PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.465.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.465.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.465.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_406						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.465.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.466 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_407)

3.466.1 Informationen

ID	TC_Funktion_IFO_14_407
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.466.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.466.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.466.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_407 PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.466.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.467 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_408)

3.467.1 Informationen

ID	TC_Funktion_IFO_14_408
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.467.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.467.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.467.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_408 PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.467.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.468 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_409)

3.468.1 Informationen

ID	TC_Funktion_IFO_14_409
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.468.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.468.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.468.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_409
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.468.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.469 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_410)

3.469.1 Informationen

ID	TC_Funktion_IFO_14_410
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.IMP_PUB, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.469.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.469.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.469.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_410						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.469.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.470 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_411)

3.470.1 Informationen

ID	TC_Funktion_IFO_14_411
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für PIN-Objekte (PIN.GW zur Speicherung der GW-System-PIN), das Kommando 'CHANGE REFERENCE DATA (Wechseln einer PIN)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.470.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.470.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.470.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_411 CHANGE REFERENCE DATA (Wechseln einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

3.470.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.471 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_412)

3.471.1 Informationen

ID	TC_Funktion_IFO_14_412
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für PIN-Objekte (PIN.GW zur Speicherung der GW-System-PIN), das Kommando 'CHANGE REFERENCE DATA (Setzen

	einer PIN)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.471.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.471.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.471.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_412						
CHANGE REFERENCE DATA (Setzen einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	01	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die neue PIN.

3.471.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.472 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_14_413)

3.472.1 Informationen

ID	TC_Funktion_IFO_14_413
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien

	und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für PIN-Objekte (PIN.GW zur Speicherung der GW-System-PIN), das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.472.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.472.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.472.4 APDU-Kommandos

ID: CM-Funktion_IFO_14_413						
GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.472.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.473 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_414)

3.473.1 Informationen

ID	TC_Funktion_IFO_16_414
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für MF, das Kommando 'CREATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.473.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.473.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.473.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_414 CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.473.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.474 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_415)

3.474.1 Informationen

ID	TC_Funktion_IFO_16_415
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für MF, das Kommando 'CREATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.474.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.474.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.474.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_415						
CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.474.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.475 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_416)

3.475.1 Informationen

ID	TC_Funktion_IFO_16_416
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für MF, das Kommando 'CREATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.475.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.475.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.475.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_416						
CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.475.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.476 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_417)

3.476.1 Informationen

ID	TC_Funktion_IFO_16_417
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für MF, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.476.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.476.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.476.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_417						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le

00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.476.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.477 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_418)

3.477.1 Informationen

ID	TC_Funktion_IFO_16_418
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für MF, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.477.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.477.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.477.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_418						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.477.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.478 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_419)

3.478.1 Informationen

ID	TC_Funktion_IFO_16_419
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für MF, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.478.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.478.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.478.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_419						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.478.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.479 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_420)

3.479.1 Informationen

ID	TC_Funktion_IFO_16_420
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für MF, das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.479.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.479.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.479.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_420						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.479.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.480 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_421)

3.480.1 Informationen

ID	TC_Funktion_IFO_16_421
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für MF, das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.480.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.480.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.480.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_421						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.480.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.481 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_422)

3.481.1 Informationen

ID	TC_Funktion_IFO_16_422
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für MF, das Kommando 'DELETE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.481.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.481.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.481.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_422						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.481.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.482 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_423)

3.482.1 Informationen

ID	TC_Funktion_IFO_16_423
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für MF, das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.482.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.482.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.482.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_423						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.482.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.483 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_424)

3.483.1 Informationen

ID	TC_Funktion_IFO_16_424
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für MF, das Kommando 'SELECT (MF)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.483.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.483.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.483.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_424						
SELECT (MF)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	00	0c	02	3f 00	--

3.483.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.484 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_425)

3.484.1 Informationen

ID	TC_Funktion_IFO_16_425
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für MF, das Kommando 'TERMINATE DF' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.484.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.484.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.484.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_425						
TERMINATE DF						
CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

3.484.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.485 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_426)

3.485.1 Informationen

ID	TC_Funktion_IFO_16_426
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für MF, das Kommando 'TERMINATE DF' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.485.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.485.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.485.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_426						
TERMINATE DF						
CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

3.485.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.486 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_427)

3.486.1 Informationen

ID	TC_Funktion_IFO_16_427
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'ACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.486.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.486.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.486.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_427						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.486.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.487 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_428)

3.487.1 Informationen

ID	TC_Funktion_IFO_16_428
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.487.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.487.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.487.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_428						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.487.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.488 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_429)

3.488.1 Informationen

ID	TC_Funktion_IFO_16_429
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.488.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.488.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.488.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_429						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.488.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.489 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_430)

3.489.1 Informationen

ID	TC_Funktion_IFO_16_430
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'CREATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.489.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.489.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.489.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_430						
CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.489.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.490 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_431)

3.490.1 Informationen

ID	TC_Funktion_IFO_16_431
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando

	'CREATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.490.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.490.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.490.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_431						
CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.490.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.491 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_432)

3.491.1 Informationen

ID	TC_Funktion_IFO_16_432
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien

	und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'CREATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.491.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.491.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.491.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_432						
CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.491.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.492 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_433)

3.492.1 Informationen

ID	TC_Funktion_IFO_16_433
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.492.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.492.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.492.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_433 CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.492.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.493 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_434)

3.493.1 Informationen

ID	TC_Funktion_IFO_16_434
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.493.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.493.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.493.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_434 CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.493.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.494 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_435)

3.494.1 Informationen

ID	TC_Funktion_IFO_16_435
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.494.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.494.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.494.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_435
CREATE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.494.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.495 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_436)

3.495.1 Informationen

ID	TC_Funktion_IFO_16_436
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.495.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.495.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.495.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_436						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.495.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.496 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_437)

3.496.1 Informationen

ID	TC_Funktion_IFO_16_437
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.496.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.496.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.496.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_437						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.496.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.497 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_438)

3.497.1 Informationen

ID	TC_Funktion_IFO_16_438
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.497.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.497.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.497.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_438						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.497.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.498 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_439)

3.498.1 Informationen

ID	TC_Funktion_IFO_16_439
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'DELETE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.498.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.498.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.498.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_439						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.498.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.499 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_440)

3.499.1 Informationen

ID	TC_Funktion_IFO_16_440
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.499.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.499.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.499.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_440						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.499.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.500 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_441)

3.500.1 Informationen

ID	TC_Funktion_IFO_16_441
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'DELETE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.500.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.500.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.500.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_441						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.500.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.501 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_442)

3.501.1 Informationen

ID	TC_Funktion_IFO_16_442
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'SELECT (DF mittels FID)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.501.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.501.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.501.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_442						
SELECT (DF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden DF.

3.501.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.502 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_443)

3.502.1 Informationen

ID	TC_Funktion_IFO_16_443
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'TERMINATE DF' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.502.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.502.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.502.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_443						
TERMINATE DF						
CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

3.502.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.503 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_444)

3.503.1 Informationen

ID	TC_Funktion_IFO_16_444
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'TERMINATE DF' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.503.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.503.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.503.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_444						
TERMINATE DF						
CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

3.503.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.504 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_445)

3.504.1 Informationen

ID	TC_Funktion_IFO_16_445
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'TERMINATE DF' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.504.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.504.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.504.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_445							
TERMINATE DF							
CLA	INS	P1	P2	Lc	Data	Le	
00	e6	00	00	--	--	--	

3.504.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.505 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_446)

3.505.1 Informationen

ID	TC_Funktion_IFO_16_446
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs, das Kommando 'ACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.505.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.505.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.505.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_446						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.505.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.506 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_447)

3.506.1 Informationen

ID	TC_Funktion_IFO_16_447
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs, das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.506.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.506.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.506.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_447						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.506.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.507 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_448)

3.507.1 Informationen

ID	TC_Funktion_IFO_16_448
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs, das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.507.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.507.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.507.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_448							
ACTIVATE FILE							
CLA	INS	P1	P2	Lc	Data	Le	
00	44	00	00	--	--	--	

3.507.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.508 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_449)

3.508.1 Informationen

ID	TC_Funktion_IFO_16_449
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs, das Kommando 'APPEND RECORD (ohne SFI)' und ohne Sicherheitszustand. Dieser Testfall ist nur gültig, sofern das Kommando im Sicherheitsmodul implementiert ist
Klassifizierung	Fehlerfall-Test

3.508.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.508.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.508.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_449 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.508.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.509 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_450)

3.509.1 Informationen

ID	TC_Funktion_IFO_16_450
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs, das Kommando 'APPEND RECORD (ohne SFI)' und den Sicherheitszustand PACE. Dieser Testfall ist nur gültig, sofern das Kommando im Sicherheitsmodul implementiert ist
Klassifizierung	Fehlerfall-Test

3.509.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.509.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.509.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_450 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.509.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.510 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_451)

3.510.1 Informationen

ID	TC_Funktion_IFO_16_451
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs, das Kommando 'APPEND RECORD (ohne SFI)' und den Sicherheitszustand PACE + AUTH. Dieser Testfall ist nur gültig, sofern das Kommando im Sicherheitsmodul implementiert ist
Klassifizierung	Gutfall-Test

3.510.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.510.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.510.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_451						
APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.510.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.511 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_452)

3.511.1 Informationen

ID	TC_Funktion_IFO_16_452
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs, das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.511.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.511.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.511.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_452						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.511.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.512 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_453)

3.512.1 Informationen

ID	TC_Funktion_IFO_16_453
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs, das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand

	PACE.
Klassifizierung	Fehlerfall-Test

3.512.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.512.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.512.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_453						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.512.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.513 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_454)

3.513.1 Informationen

ID	TC_Funktion_IFO_16_454
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF und in weiteren

	ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs, das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.513.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.513.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.513.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_454						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.513.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.514 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_455)

3.514.1 Informationen

ID	TC_Funktion_IFO_16_455
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase

	'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs, das Kommando 'DELETE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.514.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.514.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.514.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_455						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.514.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.515 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_456)

3.515.1 Informationen

ID	TC_Funktion_IFO_16_456
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das

	MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs, das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.515.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.515.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.515.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_456						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.515.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.516 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_457)

3.516.1 Informationen

ID	TC_Funktion_IFO_16_457
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien

	und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs, das Kommando 'DELETE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.516.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.516.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.516.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_457						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.516.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.517 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_458)

3.517.1 Informationen

ID	TC_Funktion_IFO_16_458

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs, das Kommando 'SELECT (EF mittels FID)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.517.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.517.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.517.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_458						
SELECT (EF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	02	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

3.517.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.518 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_459)

3.518.1 Informationen

ID	TC_Funktion_IFO_16_459
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs, das Kommando 'TERMINATE EF' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.518.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.518.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.518.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_459						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.518.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.519 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_460)

3.519.1 Informationen

ID	TC_Funktion_IFO_16_460
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs, das Kommando 'TERMINATE EF' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.519.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.519.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.519.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_460						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.519.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.520 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_461)

3.520.1 Informationen

ID	TC_Funktion_IFO_16_461
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs, das Kommando 'TERMINATE EF' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.520.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.520.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.520.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_461						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.520.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.521 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_462)

3.521.1 Informationen

ID	TC_Funktion_IFO_16_462
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs, das Kommando 'READ BINARY (ohne SFI) / READ RECORD (ohne SFI)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.521.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.521.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.521.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_462 READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

ID: CM-Funktion_IFO_16_462

READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.521.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.522 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_463)

3.522.1 Informationen

ID	TC_Funktion_IFO_16_463
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs, das Kommando 'READ BINARY (ohne SFI) / READ RECORD (ohne SFI)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.522.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.522.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.522.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_463						
READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

ID: CM-Funktion_IFO_16_463						
READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.522.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.523 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_464)

3.523.1 Informationen

ID	TC_Funktion_IFO_16_464
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs, das Kommando 'READ BINARY (ohne SFI) / READ RECORD

	(ohne SFI)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.523.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.523.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.523.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_464						
READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

ID: CM-Funktion_IFO_16_464						
READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.523.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.524 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_465)

3.524.1 Informationen

ID	TC_Funktion_IFO_16_465
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs, das Kommando 'UPDATE BINARY (ohne SFI) / UPDATE RECORD (ohne SFI)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.524.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.524.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.524.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_465 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

ID: CM-Funktion_IFO_16_465

UPDATE RECORD (ohne SFI)

CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.524.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.525 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_466)

3.525.1 Informationen

ID	TC_Funktion_IFO_16_466
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs, das Kommando 'UPDATE BINARY (ohne SFI) / UPDATE RECORD (ohne SFI)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.525.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.525.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.525.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_466 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält $(\text{Offset} - \text{P2}) / 256$, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

ID: CM-Funktion_IFO_16_466 UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.525.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.526 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_467)

3.526.1 Informationen

ID	TC_Funktion_IFO_16_467
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im MF und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des MF angelegte EFs, das Kommando 'UPDATE BINARY (ohne SFI) / UPDATE RECORD (ohne SFI)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.526.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.526.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.526.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_467 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

ID: CM-Funktion_IFO_16_467 UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.526.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.527 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_468)

3.527.1 Informationen

ID	TC_Funktion_IFO_16_468
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'ACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.527.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.527.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.527.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_468 ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.527.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.528 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_469)

3.528.1 Informationen

ID	TC_Funktion_IFO_16_469
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.528.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.528.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.528.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_469						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.528.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.529 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_470)

3.529.1 Informationen

ID	TC_Funktion_IFO_16_470
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'APPEND RECORD (ohne SFI)' und ohne Sicherheitszustand. Dieser Testfall ist nur gültig, sofern das Kommando im Sicherheitsmodul implementiert ist
Klassifizierung	Fehlerfall-Test

3.529.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.529.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.529.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_470 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.529.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.530 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_471)

3.530.1 Informationen

ID	TC_Funktion_IFO_16_471
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'APPEND RECORD (ohne SFI)' und den

	Sicherheitszustand PACE. Dieser Testfall ist nur gültig, sofern das Kommando im Sicherheitsmodul implementiert ist
Klassifizierung	Fehlerfall-Test

3.530.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.530.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.530.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_471 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.530.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.531 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_472)

3.531.1 Informationen

ID	TC_Funktion_IFO_16_472
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien

	und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.531.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.531.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.531.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_472						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.531.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.532 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_473)

3.532.1 Informationen

ID	TC_Funktion_IFO_16_473

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.532.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.532.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.532.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_473						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.532.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.533 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_474)

3.533.1 Informationen

ID	TC_Funktion_IFO_16_474
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'DELETE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.533.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.533.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.533.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_474						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.533.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.534 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_475)

3.534.1 Informationen

ID	TC_Funktion_IFO_16_475
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.534.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.534.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.534.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_475						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.534.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.535 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_476)

3.535.1 Informationen

ID	TC_Funktion_IFO_16_476
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'READ RECORD (ohne SFI)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.535.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.535.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.535.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_476 READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.535.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.536 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_477)

3.536.1 Informationen

ID	TC_Funktion_IFO_16_477
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'SELECT (EF mittels FID)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.536.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.536.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.536.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_477 SELECT (EF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	02	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

3.536.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.537 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_478)

3.537.1 Informationen

ID	TC_Funktion_IFO_16_478
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'TERMINATE EF' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.537.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.537.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.537.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_478							
TERMINATE EF							
CLA	INS	P1	P2	Lc	Data		Le

00	e8	00	00	--	--	--

3.537.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.538 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_479)

3.538.1 Informationen

ID	TC_Funktion_IFO_16_479
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'TERMINATE EF' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.538.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.538.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.538.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_479
TERMINATE EF

CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.538.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.539 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_480)

3.539.1 Informationen

ID	TC_Funktion_IFO_16_480
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'UPDATE RECORD (ohne SFI)' und ohne Sicherheitszustand. Dieser Testfall ist nur gültig, wenn das Sicherheitsmodul nicht die Funktionalität des Sicherheitsmodul-Firmware-Updates bietet (in diesem Fall gelten die Zugriffsregeln für ein Update des Datenfeldes wie im Rahmen des Firmware-Updates vorgesehen)
Klassifizierung	Fehlerfall-Test

3.539.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.539.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.539.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_480						
UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.539.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.540 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_481)

3.540.1 Informationen

ID	TC_Funktion_IFO_16_481
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModTRInfo (Technisches Datenfeld mit Informationen zu der für das vorliegende Sicherheitsmodul relevanten Spezifikation), das Kommando 'UPDATE RECORD (ohne SFI)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.540.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.540.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.540.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_481 UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.540.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.541 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_482)

3.541.1 Informationen

ID	TC_Funktion_IFO_16_482
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModAccess (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen PACE-Funktionalität), das Kommando 'ACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.541.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.541.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.541.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_482						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.541.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.542 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_483)

3.542.1 Informationen

ID	TC_Funktion_IFO_16_483
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModAccess (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen PACE-Funktionalität), das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.542.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.542.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.542.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_483						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.542.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.543 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_484)

3.543.1 Informationen

ID	TC_Funktion_IFO_16_484
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModAccess (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen PACE-Funktionalität), das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.543.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.543.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.543.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_484						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.543.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.544 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_485)

3.544.1 Informationen

ID	TC_Funktion_IFO_16_485
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModAccess (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen PACE-Funktionalität), das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.544.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.544.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.544.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_485						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.544.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.545 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_486)

3.545.1 Informationen

ID	TC_Funktion_IFO_16_486
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModAccess (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen PACE-Funktionalität), das Kommando 'DELETE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.545.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.545.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.545.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_486						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.545.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.546 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_487)

3.546.1 Informationen

ID	TC_Funktion_IFO_16_487
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModAccess (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen PACE-Funktionalität), das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.546.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.546.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.546.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_487						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.546.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.547 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_488)

3.547.1 Informationen

ID	TC_Funktion_IFO_16_488
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModAccess (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen PACE-Funktionalität), das Kommando 'READ BINARY (ohne SFI)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.547.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.547.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.547.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_488						
READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.547.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.548 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_489)

3.548.1 Informationen

ID	TC_Funktion_IFO_16_489
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModAccess (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen

	PACE-Funktionalität), das Kommando 'SELECT (EF mittels FID)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.548.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.548.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.548.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_489						
SELECT (EF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	02	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

3.548.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.549 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_490)

3.549.1 Informationen

ID	TC_Funktion_IFO_16_490
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das

	MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModAccess (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen PACE-Funktionalität), das Kommando 'TERMINATE EF' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.549.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.549.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.549.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_490						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.549.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.550 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_491)

3.550.1 Informationen

ID	TC_Funktion_IFO_16_491

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModAccess (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen PACE-Funktionalität), das Kommando 'TERMINATE EF' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.550.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.550.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.550.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_491						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.550.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.551 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_492)

3.551.1 Informationen

ID	TC_Funktion_IFO_16_492
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModAccess (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen PACE-Funktionalität), das Kommando 'UPDATE BINARY (ohne SFI)' und ohne Sicherheitszustand. Dieser Testfall ist nur gültig, wenn das Sicherheitsmodul nicht die Funktionalität des Sicherheitsmodul-Firmware-Updates bietet (in diesem Fall gelten die Zugriffsregeln für ein Update des Datenfeldes wie im Rahmen des Firmware-Updates vorgesehen)
Klassifizierung	Fehlerfall-Test

3.551.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.551.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.551.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_492 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.551.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.552 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_493)

3.552.1 Informationen

ID	TC_Funktion_IFO_16_493
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModAccess (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen PACE-Funktionalität), das Kommando 'UPDATE BINARY (ohne SFI)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.552.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.552.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.552.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_493						
UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le

00	d6	XX	XX	LL	XX...XX	--

'P1' enthält $(\text{Offset} - P2) / 256$, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.552.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.553 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_494)

3.553.1 Informationen

ID	TC_Funktion_IFO_16_494
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität), das Kommando 'ACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.553.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.553.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.553.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_494						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.553.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.554 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_495)

3.554.1 Informationen

ID	TC_Funktion_IFO_16_495
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität), das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.554.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.554.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.554.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_495						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.554.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.555 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_496)

3.555.1 Informationen

ID	TC_Funktion_IFO_16_496
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität), das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.555.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.555.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.555.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_496							
DEACTIVATE FILE							
CLA	INS	P1	P2	Lc	Data	Le	
00	04	00	00	--	--	--	

3.555.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.556 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_497)

3.556.1 Informationen

ID	TC_Funktion_IFO_16_497
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität), das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.556.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.556.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.556.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_497						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.556.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.557 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_498)

3.557.1 Informationen

ID	TC_Funktion_IFO_16_498
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität), das Kommando 'DELETE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.557.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.557.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.557.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_498						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.557.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.558 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_499)

3.558.1 Informationen

ID	TC_Funktion_IFO_16_499
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität), das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.558.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.558.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.558.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_499						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.558.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.559 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_500)

3.559.1 Informationen

ID	TC_Funktion_IFO_16_500
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität), das Kommando 'READ BINARY (ohne SFI)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.559.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.559.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.559.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_500						
READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.559.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.560 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_501)

3.560.1 Informationen

ID	TC_Funktion_IFO_16_501
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität), das Kommando 'SELECT (EF mittels FID)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.560.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.560.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.560.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_501 SELECT (EF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	02	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

3.560.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.561 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_502)

3.561.1 Informationen

ID	TC_Funktion_IFO_16_502
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität), das Kommando 'TERMINATE EF' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.561.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.561.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.561.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_502						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.561.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.562 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_503)

3.562.1 Informationen

ID	TC_Funktion_IFO_16_503
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität), das Kommando 'TERMINATE EF' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.562.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.562.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.562.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_503						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.562.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.563 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_504)

3.563.1 Informationen

ID	TC_Funktion_IFO_16_504
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität), das Kommando 'UPDATE BINARY (ohne SFI)' und ohne Sicherheitszustand. Dieser Testfall ist nur gültig, wenn das Sicherheitsmodul nicht die Funktionalität des Sicherheitsmodul-Firmware-Updates bietet (in diesem Fall gelten die Zugriffsregeln für ein Update des

	Datenfeldes wie im Rahmen des Firmware-Updates vorgesehen)
Klassifizierung	Fehlerfall-Test

3.563.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.563.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.563.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_504 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.563.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.564 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_505)

3.564.1 Informationen

ID	TC_Funktion_IFO_16_505

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModCrypto (Technisches Datenfeld mit Informationen zu der vom vorliegenden Sicherheitsmodul angebotenen Krypto-Funktionalität), das Kommando 'UPDATE BINARY (ohne SFI)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.564.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.564.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.564.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_505						
UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.564.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.565 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_506)

3.565.1 Informationen

ID	TC_Funktion_IFO_16_506
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls), das Kommando 'ACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.565.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.565.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.565.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_506						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.565.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.566 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_507)

3.566.1 Informationen

ID	TC_Funktion_IFO_16_507
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls), das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.566.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.566.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.566.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_507						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.566.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.567 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_508)

3.567.1 Informationen

ID	TC_Funktion_IFO_16_508
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls), das Kommando 'APPEND RECORD (ohne SFI)' und ohne Sicherheitszustand. Dieser Testfall ist nur gültig, sofern das Kommando im Sicherheitsmodul implementiert ist
Klassifizierung	Fehlerfall-Test

3.567.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.567.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.567.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_508 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.567.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.568 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_509)

3.568.1 Informationen

ID	TC_Funktion_IFO_16_509
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls), das Kommando 'APPEND RECORD (ohne SFI)' und den Sicherheitszustand PACE. Dieser Testfall ist nur gültig, sofern das Kommando im Sicherheitsmodul implementiert ist
Klassifizierung	Fehlerfall-Test

3.568.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.568.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.568.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_509 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le

00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.568.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.569 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_510)

3.569.1 Informationen

ID	TC_Funktion_IFO_16_510
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls), das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.569.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.569.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.569.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_510						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.569.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.570 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_511)

3.570.1 Informationen

ID	TC_Funktion_IFO_16_511
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls), das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.570.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.570.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.570.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_511 DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.570.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.571 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_512)

3.571.1 Informationen

ID	TC_Funktion_IFO_16_512
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls), das Kommando 'DELETE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.571.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.571.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.571.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_512						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.571.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.572 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_513)

3.572.1 Informationen

ID	TC_Funktion_IFO_16_513
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls), das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.572.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.572.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.572.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_513						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.572.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.573 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_514)

3.573.1 Informationen

ID	TC_Funktion_IFO_16_514
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls), das Kommando 'READ RECORD (ohne SFI)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.573.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.573.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.573.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_514						
READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.573.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.574 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_515)

3.574.1 Informationen

ID	TC_Funktion_IFO_16_515
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls), das Kommando 'READ RECORD (ohne SFI)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.574.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.574.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.574.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_515						
READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.574.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.575 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_516)

3.575.1 Informationen

ID	TC_Funktion_IFO_16_516
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls), das Kommando 'SELECT (EF mittels FID)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.575.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.575.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.575.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_516						
SELECT (EF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	02	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

3.575.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.576 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_517)

3.576.1 Informationen

ID	TC_Funktion_IFO_16_517
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls), das Kommando 'TERMINATE EF' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.576.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.576.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.576.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_517						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.576.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.577 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_518)

3.577.1 Informationen

ID	TC_Funktion_IFO_16_518
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls), das Kommando 'TERMINATE EF' und den

	Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.577.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.577.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.577.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_518						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.577.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.578 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_519)

3.578.1 Informationen

ID	TC_Funktion_IFO_16_519
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModLifeCycle (Technisches Datenfeld

	mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls), das Kommando 'UPDATE RECORD (ohne SFI)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.578.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.578.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.578.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_519 UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.578.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.579 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_520)

3.579.1 Informationen

ID	TC_Funktion_IFO_16_520
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SecModLifeCycle (Technisches Datenfeld mit Informationen zum Life Cycle-Status des vorliegenden Sicherheitsmoduls), das Kommando 'UPDATE RECORD (ohne SFI)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.579.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.579.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.579.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_520 UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.579.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.580 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_521)

3.580.1 Informationen

ID	TC_Funktion_IFO_16_521
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für PIN.GW zur Speicherung der GW-System-PIN, das Kommando 'CHANGE REFERENCE DATA (Wechseln einer PIN)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.580.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.580.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.580.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_521 CHANGE REFERENCE DATA (Wechseln einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

3.580.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.581 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_522)

3.581.1 Informationen

ID	TC_Funktion_IFO_16_522
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für PIN.GW zur Speicherung der GW-System-PIN, das Kommando 'CHANGE REFERENCE DATA (Wechseln einer PIN)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.581.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.581.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.581.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_522
CHANGE REFERENCE DATA (Wechseln einer PIN)

CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

3.581.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.582 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_523)

3.582.1 Informationen

ID	TC_Funktion_IFO_16_523
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für PIN.GW zur Speicherung der GW-System-PIN, das Kommando 'CHANGE REFERENCE DATA (Setzen einer PIN)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.582.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.582.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.582.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_523						
CHANGE REFERENCE DATA (Setzen einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	01	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die neue PIN.

3.582.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.583 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_524)

3.583.1 Informationen

ID	TC_Funktion_IFO_16_524
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für PIN.GW zur Speicherung der GW-System-PIN, das Kommando 'CHANGE REFERENCE DATA (Setzen einer PIN)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.583.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.583.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.583.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_524						
CHANGE REFERENCE DATA (Setzen einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	01	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die neue PIN.

3.583.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.584 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_525)

3.584.1 Informationen

ID	TC_Funktion_IFO_16_525
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für PIN.GW zur Speicherung der GW-System-PIN, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.584.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.584.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.584.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_525						
GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.584.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.585 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_526)

3.585.1 Informationen

ID	TC_Funktion_IFO_16_526
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase

	'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.585.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.585.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.585.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_526						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.585.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.586 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_527)

3.586.1 Informationen

ID	TC_Funktion_IFO_16_527
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.586.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.586.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.586.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_527						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.586.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.587 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_528)

3.587.1 Informationen

ID	TC_Funktion_IFO_16_528
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.587.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.587.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.587.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_528 ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.587.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.588 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_529)

3.588.1 Informationen

ID	TC_Funktion_IFO_16_529
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.588.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.588.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.588.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_529
CREATE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.588.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.589 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_530)

3.589.1 Informationen

ID	TC_Funktion_IFO_16_530
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.589.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.589.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.589.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_530						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.589.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.590 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_531)

3.590.1 Informationen

ID	TC_Funktion_IFO_16_531
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.590.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.590.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.590.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_531						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.590.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.591 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_532)

3.591.1 Informationen

ID	TC_Funktion_IFO_16_532
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.591.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.591.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.591.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_532						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.591.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.592 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_533)

3.592.1 Informationen

ID	TC_Funktion_IFO_16_533
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die

	Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.592.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.592.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.592.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_533						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.592.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.593 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_534)

3.593.1 Informationen

ID	TC_Funktion_IFO_16_534
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.593.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.593.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.593.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_534						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.593.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.594 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_535)

3.594.1 Informationen

ID	TC_Funktion_IFO_16_535
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.594.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.594.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.594.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_535 DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.594.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.595 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_536)

3.595.1 Informationen

ID	TC_Funktion_IFO_16_536
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.595.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.595.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.595.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_536 DELETE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.595.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.596 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_537)

3.596.1 Informationen

ID	TC_Funktion_IFO_16_537
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.596.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.596.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.596.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_537						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.596.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.597 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_538)

3.597.1 Informationen

ID	TC_Funktion_IFO_16_538
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.597.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.597.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.597.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_538 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.597.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.598 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_539)

3.598.1 Informationen

ID	TC_Funktion_IFO_16_539
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.598.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.598.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.598.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_539						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.598.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.599 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_540)

3.599.1 Informationen

ID	TC_Funktion_IFO_16_540
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die

	Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.599.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.599.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.599.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_540						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.599.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.600 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_541)

3.600.1 Informationen

ID	TC_Funktion_IFO_16_541
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.600.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.600.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.600.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_541 GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator

sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.600.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.601 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_542)

3.601.1 Informationen

ID	TC_Funktion_IFO_16_542
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.601.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.601.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.601.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_542						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le

00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.601.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.602 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_543)

3.602.1 Informationen

ID	TC_Funktion_IFO_16_543
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.602.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.602.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.602.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_543 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.602.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.603 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_544)

3.603.1 Informationen

ID	TC_Funktion_IFO_16_544
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.603.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.603.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.603.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_544 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.603.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.604 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_545)

3.604.1 Informationen

ID	TC_Funktion_IFO_16_545
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase

	'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.604.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.604.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.604.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_545						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.604.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.605 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_546)

3.605.1 Informationen

ID	TC_Funktion_IFO_16_546
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.605.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.605.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.605.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_546 GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.605.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.606 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_547)

3.606.1 Informationen

ID	TC_Funktion_IFO_16_547
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.606.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.606.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.606.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_547 GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.606.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.607 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_548)

3.607.1 Informationen

ID	TC_Funktion_IFO_16_548
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.607.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.607.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.607.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_548

GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.607.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.608 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_549)

3.608.1 Informationen

ID	TC_Funktion_IFO_16_549
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.608.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.608.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.608.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_549						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.608.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.609 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_550)

3.609.1 Informationen

ID	TC_Funktion_IFO_16_550

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.609.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.609.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.609.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_550						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.609.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.610 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_551)

3.610.1 Informationen

ID	TC_Funktion_IFO_16_551
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.610.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.610.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.610.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_551 INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.610.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.611 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_552)

3.611.1 Informationen

ID	TC_Funktion_IFO_16_552
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.611.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.611.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.611.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_552 INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.611.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.612 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_553)

3.612.1 Informationen

ID	TC_Funktion_IFO_16_553
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.612.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.612.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.612.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_553						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le

00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.612.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.613 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_554)

3.613.1 Informationen

ID	TC_Funktion_IFO_16_554
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.613.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.613.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.613.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_554

PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.613.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.614 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_555)

3.614.1 Informationen

ID	TC_Funktion_IFO_16_555
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.614.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.614.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.614.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_555						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.614.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.615 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_556)

3.615.1 Informationen

ID	TC_Funktion_IFO_16_556
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.615.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.615.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.615.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_556						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.615.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.616 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_557)

3.616.1 Informationen

ID	TC_Funktion_IFO_16_557
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien

	und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.616.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.616.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.616.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_557						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.616.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.617 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_558)

3.617.1 Informationen

ID	TC_Funktion_IFO_16_558
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.617.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.617.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.617.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_558						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.617.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.618 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_559)

3.618.1 Informationen

ID	TC_Funktion_IFO_16_559
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'activated')' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.618.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.618.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.618.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_559 PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'activated')						
CLA	INS	P1	P2	Lc	Data	Le

00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.618.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.619 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_560)

3.619.1 Informationen

ID	TC_Funktion_IFO_16_560
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'deactivated')' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.619.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.619.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.619.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_560 PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'deactivated')						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.619.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.620 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_561)

3.620.1 Informationen

ID	TC_Funktion_IFO_16_561
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'deactivated')' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.620.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.620.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.620.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_561 PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'deactivated')						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.620.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.621 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_562)

3.621.1 Informationen

ID	TC_Funktion_IFO_16_562
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das

	MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'initialisation')' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.621.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.621.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.621.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_562						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'initialisation')						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.621.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.622 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_563)

3.622.1 Informationen

ID	TC_Funktion_IFO_16_563
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'initialisation')' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.622.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.622.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.622.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_563 PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'initialisation')						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.622.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.623 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_564)

3.623.1 Informationen

ID	TC_Funktion_IFO_16_564
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.623.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.623.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.623.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_564 ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.623.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.624 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_565)

3.624.1 Informationen

ID	TC_Funktion_IFO_16_565
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.624.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.624.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.624.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_565
ACTIVATE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.624.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.625 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_566)

3.625.1 Informationen

ID	TC_Funktion_IFO_16_566
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.625.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.625.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.625.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_566						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.625.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.626 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_567)

3.626.1 Informationen

ID	TC_Funktion_IFO_16_567
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.626.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.626.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.626.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_567						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.626.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.627 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_568)

3.627.1 Informationen

ID	TC_Funktion_IFO_16_568
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.627.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.627.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.627.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_568						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.627.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.628 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_569)

3.628.1 Informationen

ID	TC_Funktion_IFO_16_569
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando

	'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.628.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.628.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.628.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_569						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.628.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.629 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_570)

3.629.1 Informationen

ID	TC_Funktion_IFO_16_570

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.629.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.629.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.629.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_570						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.629.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.630 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_571)

3.630.1 Informationen

ID	TC_Funktion_IFO_16_571
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.630.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.630.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.630.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_571						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.630.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.631 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_572)

3.631.1 Informationen

ID	TC_Funktion_IFO_16_572
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.631.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.631.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.631.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_572						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.631.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.632 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_573)

3.632.1 Informationen

ID	TC_Funktion_IFO_16_573
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.632.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.632.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.632.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_573
DELETE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.632.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.633 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_574)

3.633.1 Informationen

ID	TC_Funktion_IFO_16_574
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.633.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.633.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.633.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_574						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.633.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.634 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_575)

3.634.1 Informationen

ID	TC_Funktion_IFO_16_575
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.634.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.634.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.634.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_575						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.634.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.635 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_576)

3.635.1 Informationen

ID	TC_Funktion_IFO_16_576
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.635.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.635.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.635.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_576 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.635.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.636 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_577)

3.636.1 Informationen

ID	TC_Funktion_IFO_16_577
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.636.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.636.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.636.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_577						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.636.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.637 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_578)

3.637.1 Informationen

ID	TC_Funktion_IFO_16_578
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.637.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.637.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.637.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_578 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit

SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.637.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.638 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_579)

3.638.1 Informationen

ID	TC_Funktion_IFO_16_579
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.638.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.638.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.638.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_579						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le

00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.638.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.639 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_580)

3.639.1 Informationen

ID	TC_Funktion_IFO_16_580
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.639.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.639.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.639.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_580						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.639.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.640 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_581)

3.640.1 Informationen

ID	TC_Funktion_IFO_16_581
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase

	'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.640.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.640.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.640.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_581 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.640.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.641 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_582)

3.641.1 Informationen

ID	TC_Funktion_IFO_16_582
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.641.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.641.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.641.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_582 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.641.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.642 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_583)

3.642.1 Informationen

ID	TC_Funktion_IFO_16_583
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.642.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.642.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.642.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_583						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.642.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.643 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_584)

3.643.1 Informationen

ID	TC_Funktion_IFO_16_584
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.643.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.643.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.643.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_584
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.643.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.644 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_585)

3.644.1 Informationen

ID	TC_Funktion_IFO_16_585
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.644.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.644.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.644.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_585						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.644.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.645 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_586)

3.645.1 Informationen

ID	TC_Funktion_IFO_16_586
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.645.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.645.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.645.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_586						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.645.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.646 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_587)

3.646.1 Informationen

ID	TC_Funktion_IFO_16_587
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das

	MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.646.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.646.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.646.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_587						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.646.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.647 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_588)

3.647.1 Informationen

ID	TC_Funktion_IFO_16_588
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.647.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.647.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.647.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_588						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu

generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'
Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.647.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.648 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_589)

3.648.1 Informationen

ID	TC_Funktion_IFO_16_589
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.648.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.648.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.648.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_589 INTERNAL AUTHENTICATE

CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.648.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.649 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_590)

3.649.1 Informationen

ID	TC_Funktion_IFO_16_590
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.649.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.649.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.649.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_590						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.649.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.650 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_591)

3.650.1 Informationen

ID	TC_Funktion_IFO_16_591
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.650.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.650.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.650.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_591						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.650.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.651 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_592)

3.651.1 Informationen

ID	TC_Funktion_IFO_16_592
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.651.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.651.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.651.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_592						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.651.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.652 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_593)

3.652.1 Informationen

ID	TC_Funktion_IFO_16_593
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.652.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.652.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.652.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_593						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.652.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.653 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_594)

3.653.1 Informationen

ID	TC_Funktion_IFO_16_594
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.653.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.653.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.653.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_594 PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.653.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.654 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_595)

3.654.1 Informationen

ID	TC_Funktion_IFO_16_595
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.654.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.654.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.654.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_595 PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.654.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.655 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_596)

3.655.1 Informationen

ID	TC_Funktion_IFO_16_596
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.655.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.655.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.655.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_596
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.655.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.656 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_597)

3.656.1 Informationen

ID	TC_Funktion_IFO_16_597
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'activated')' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.656.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.656.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.656.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_597 PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'activated')						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.656.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.657 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_598)

3.657.1 Informationen

ID	TC_Funktion_IFO_16_598
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'deactivated')' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.657.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.657.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.657.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_598 PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'deactivated')						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.657.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.658 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_599)

3.658.1 Informationen

ID	TC_Funktion_IFO_16_599
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das

	MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'deactivated')' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.658.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.658.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.658.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_599						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'deactivated')						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.658.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.659 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_600)

3.659.1 Informationen

ID	TC_Funktion_IFO_16_600
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'initialisation')' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.659.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.659.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.659.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_600 PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'initialisation')						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.659.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.660 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_601)

3.660.1 Informationen

ID	TC_Funktion_IFO_16_601
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_TLS_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'initialisation')' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.660.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.660.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.660.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_601 PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'initialisation')						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.660.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.661 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_602)

3.661.1 Informationen

ID	TC_Funktion_IFO_16_602
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.661.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.661.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.661.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_602						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.661.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.662 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_603)

3.662.1 Informationen

ID	TC_Funktion_IFO_16_603
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.662.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.662.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.662.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_603						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.662.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.663 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_604)

3.663.1 Informationen

ID	TC_Funktion_IFO_16_604
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.663.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.663.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.663.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_604						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.663.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.664 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_605)

3.664.1 Informationen

ID	TC_Funktion_IFO_16_605
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die

	Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.664.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.664.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.664.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_605						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.664.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.665 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_606)

3.665.1 Informationen

ID	TC_Funktion_IFO_16_606

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.665.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.665.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.665.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_606						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.665.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.666 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_607)

3.666.1 Informationen

ID	TC_Funktion_IFO_16_607
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.666.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.666.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.666.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_607 DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.666.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.667 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_608)

3.667.1 Informationen

ID	TC_Funktion_IFO_16_608
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.667.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.667.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.667.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_608 DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.667.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.668 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_609)

3.668.1 Informationen

ID	TC_Funktion_IFO_16_609
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.668.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.668.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.668.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_609
DEACTIVATE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.668.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.669 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_610)

3.669.1 Informationen

ID	TC_Funktion_IFO_16_610
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.669.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.669.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.669.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_610						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.669.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.670 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_611)

3.670.1 Informationen

ID	TC_Funktion_IFO_16_611
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.670.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.670.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.670.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_611						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.670.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.671 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_612)

3.671.1 Informationen

ID	TC_Funktion_IFO_16_612
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.671.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.671.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.671.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_612						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.671.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.672 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_613)

3.672.1 Informationen

ID	TC_Funktion_IFO_16_613
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die

	Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.672.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.672.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.672.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_613 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.672.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.673 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_614)

3.673.1 Informationen

ID	TC_Funktion_IFO_16_614
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien

	und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.673.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.673.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.673.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_614 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.673.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.674 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_615)

3.674.1 Informationen

ID	TC_Funktion_IFO_16_615
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.674.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.674.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.674.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_615 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit

SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.674.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.675 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_616)

3.675.1 Informationen

ID	TC_Funktion_IFO_16_616
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.675.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.675.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.675.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_616						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le

00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.675.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.676 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_617)

3.676.1 Informationen

ID	TC_Funktion_IFO_16_617
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.676.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.676.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.676.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_617						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.676.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.677 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_618)

3.677.1 Informationen

ID	TC_Funktion_IFO_16_618
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.

Klassifizierung	Fehlerfall-Test

3.677.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.677.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.677.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_618						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.677.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.678 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_619)

3.678.1 Informationen

ID	TC_Funktion_IFO_16_619
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.678.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.678.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.678.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_619 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.678.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.679 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_620)

3.679.1 Informationen

ID	TC_Funktion_IFO_16_620
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.679.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.679.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.679.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_620 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.679.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.680 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_621)

3.680.1 Informationen

ID	TC_Funktion_IFO_16_621
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.680.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.680.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.680.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_621						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.680.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.681 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_622)

3.681.1 Informationen

ID	TC_Funktion_IFO_16_622
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.681.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.681.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.681.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_622						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.681.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.682 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_623)

3.682.1 Informationen

ID	TC_Funktion_IFO_16_623
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.682.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.682.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.682.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_623						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.682.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.683 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_624)

3.683.1 Informationen

ID	TC_Funktion_IFO_16_624
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das

	MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.683.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.683.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.683.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_624						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.683.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.684 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_625)

3.684.1 Informationen

ID	TC_Funktion_IFO_16_625
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.684.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.684.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.684.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_625						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu

generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'
Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.684.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.685 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_626)

3.685.1 Informationen

ID	TC_Funktion_IFO_16_626
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.685.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.685.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.685.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_626
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.685.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.686 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_627)

3.686.1 Informationen

ID	TC_Funktion_IFO_16_627
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.686.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.686.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.686.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_627 INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.686.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.687 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_628)

3.687.1 Informationen

ID	TC_Funktion_IFO_16_628
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.687.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.687.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.687.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_628						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.687.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.688 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_629)

3.688.1 Informationen

ID	TC_Funktion_IFO_16_629
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.688.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.688.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.688.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_629 PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.688.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.689 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_630)

3.689.1 Informationen

ID	TC_Funktion_IFO_16_630
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das

	MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.689.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.689.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.689.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_630						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.689.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.690 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_631)

3.690.1 Informationen

ID	TC_Funktion_IFO_16_631
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.690.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.690.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.690.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_631 PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.690.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.691 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_632)

3.691.1 Informationen

ID	TC_Funktion_IFO_16_632
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.691.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.691.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.691.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_632						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.691.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.692 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_633)

3.692.1 Informationen

ID	TC_Funktion_IFO_16_633
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.692.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.692.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.692.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_633						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.692.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.693 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_634)

3.693.1 Informationen

ID	TC_Funktion_IFO_16_634
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.693.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.693.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.693.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_634						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.693.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.694 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_635)

3.694.1 Informationen

ID	TC_Funktion_IFO_16_635
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'PSO

	VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.694.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.694.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.694.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_635						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.694.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.695 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_636)

3.695.1 Informationen

ID	TC_Funktion_IFO_16_636

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.695.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.695.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.695.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_636						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.695.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.696 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_637)

3.696.1 Informationen

ID	TC_Funktion_IFO_16_637
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.696.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.696.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.696.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_637						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.696.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.697 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_638)

3.697.1 Informationen

ID	TC_Funktion_IFO_16_638
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.697.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.697.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.697.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_638						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.697.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.698 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_639)

3.698.1 Informationen

ID	TC_Funktion_IFO_16_639
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.698.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.698.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.698.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_639
ACTIVATE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.698.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.699 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_640)

3.699.1 Informationen

ID	TC_Funktion_IFO_16_640
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.699.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.699.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.699.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_640						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.699.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.700 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_641)

3.700.1 Informationen

ID	TC_Funktion_IFO_16_641
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.700.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.700.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.700.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_641						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.700.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.701 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_642)

3.701.1 Informationen

ID	TC_Funktion_IFO_16_642
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.701.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.701.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.701.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_642						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.701.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.702 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_643)

3.702.1 Informationen

ID	TC_Funktion_IFO_16_643
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando

	'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.702.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.702.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.702.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_643						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.702.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.703 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_644)

3.703.1 Informationen

ID	TC_Funktion_IFO_16_644

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.703.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.703.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.703.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_644						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.703.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.704 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_645)

3.704.1 Informationen

ID	TC_Funktion_IFO_16_645
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.704.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.704.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.704.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_645						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.704.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.705 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_646)

3.705.1 Informationen

ID	TC_Funktion_IFO_16_646
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.705.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.705.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.705.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_646						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.705.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.706 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_647)

3.706.1 Informationen

ID	TC_Funktion_IFO_16_647
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.706.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.706.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.706.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_647
DELETE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.706.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.707 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_648)

3.707.1 Informationen

ID	TC_Funktion_IFO_16_648
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.707.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.707.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.707.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_648						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.707.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.708 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_649)

3.708.1 Informationen

ID	TC_Funktion_IFO_16_649
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.708.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.708.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.708.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_649						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.708.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.709 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_650)

3.709.1 Informationen

ID	TC_Funktion_IFO_16_650
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.709.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.709.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.709.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_650						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.709.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.710 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_651)

3.710.1 Informationen

ID	TC_Funktion_IFO_16_651
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.710.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.710.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.710.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_651						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.710.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.711 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_652)

3.711.1 Informationen

ID	TC_Funktion_IFO_16_652
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.711.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.711.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.711.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_652 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit

SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.711.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.712 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_653)

3.712.1 Informationen

ID	TC_Funktion_IFO_16_653
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.712.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.712.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.712.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_653						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le

00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.712.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.713 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_654)

3.713.1 Informationen

ID	TC_Funktion_IFO_16_654
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.713.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.713.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.713.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_654						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.713.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.714 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_655)

3.714.1 Informationen

ID	TC_Funktion_IFO_16_655
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase

	'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.714.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.714.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.714.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_655 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.714.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.715 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_656)

3.715.1 Informationen

ID	TC_Funktion_IFO_16_656
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.715.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.715.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.715.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_656 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.715.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.716 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_657)

3.716.1 Informationen

ID	TC_Funktion_IFO_16_657
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.716.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.716.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.716.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_657 GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.716.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.717 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_658)

3.717.1 Informationen

ID	TC_Funktion_IFO_16_658
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.717.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.717.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.717.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_658
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.717.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.718 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_659)

3.718.1 Informationen

ID	TC_Funktion_IFO_16_659
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.718.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.718.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.718.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_659						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.718.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.719 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_660)

3.719.1 Informationen

ID	TC_Funktion_IFO_16_660
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.719.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.719.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.719.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_660						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.719.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.720 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_661)

3.720.1 Informationen

ID	TC_Funktion_IFO_16_661
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das

	MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.720.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.720.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.720.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_661						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.720.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.721 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_662)

3.721.1 Informationen

ID	TC_Funktion_IFO_16_662
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.721.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.721.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.721.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_662						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu

generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'
Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.721.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.722 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_663)

3.722.1 Informationen

ID	TC_Funktion_IFO_16_663
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.722.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.722.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.722.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_663 INTERNAL AUTHENTICATE

CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.722.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.723 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_664)

3.723.1 Informationen

ID	TC_Funktion_IFO_16_664
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.723.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.723.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.723.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_664						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.723.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.724 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_665)

3.724.1 Informationen

ID	TC_Funktion_IFO_16_665
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.724.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.724.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.724.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_665 PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.724.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.725 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_666)

3.725.1 Informationen

ID	TC_Funktion_IFO_16_666
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.725.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.725.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.725.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_666						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.725.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.726 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_667)

3.726.1 Informationen

ID	TC_Funktion_IFO_16_667
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.726.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.726.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.726.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_667 PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.726.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.727 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_668)

3.727.1 Informationen

ID	TC_Funktion_IFO_16_668
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.727.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.727.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.727.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_668						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.727.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.728 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_669)

3.728.1 Informationen

ID	TC_Funktion_IFO_16_669
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.728.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.728.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.728.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_669 PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.728.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.729 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_670)

3.729.1 Informationen

ID	TC_Funktion_IFO_16_670
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.729.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.729.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.729.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_670						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.729.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.730 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_671)

3.730.1 Informationen

ID	TC_Funktion_IFO_16_671
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.730.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.730.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.730.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_671						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.730.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.731 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_672)

3.731.1 Informationen

ID	TC_Funktion_IFO_16_672
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.731.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.731.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.731.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_672						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.731.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.732 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_673)

3.732.1 Informationen

ID	TC_Funktion_IFO_16_673
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase

	'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_SIG_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.732.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.732.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.732.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_673						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.732.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.733 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_674)

3.733.1 Informationen

ID	TC_Funktion_IFO_16_674
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.733.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.733.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.733.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_674 ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.733.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.734 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_675)

3.734.1 Informationen

ID	TC_Funktion_IFO_16_675
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.734.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.734.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.734.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_675						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.734.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.735 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_676)

3.735.1 Informationen

ID	TC_Funktion_IFO_16_676
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.735.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.735.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.735.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_676
ACTIVATE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.735.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.736 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_677)

3.736.1 Informationen

ID	TC_Funktion_IFO_16_677
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.736.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.736.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.736.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_677						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.736.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.737 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_678)

3.737.1 Informationen

ID	TC_Funktion_IFO_16_678
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.737.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.737.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.737.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_678						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.737.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.738 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_679)

3.738.1 Informationen

ID	TC_Funktion_IFO_16_679
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.738.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.738.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.738.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_679						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.738.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.739 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_680)

3.739.1 Informationen

ID	TC_Funktion_IFO_16_680
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die

	Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.739.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.739.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.739.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_680						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.739.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.740 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_681)

3.740.1 Informationen

ID	TC_Funktion_IFO_16_681
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.740.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.740.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.740.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_681 DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.740.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.741 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_682)

3.741.1 Informationen

ID	TC_Funktion_IFO_16_682
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.741.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.741.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.741.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_682						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.741.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.742 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_683)

3.742.1 Informationen

ID	TC_Funktion_IFO_16_683
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.742.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.742.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.742.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_683
DELETE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.742.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.743 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_684)

3.743.1 Informationen

ID	TC_Funktion_IFO_16_684
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.743.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.743.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.743.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_684						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.743.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.744 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_685)

3.744.1 Informationen

ID	TC_Funktion_IFO_16_685
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.744.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.744.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.744.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_685						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.744.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.745 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_686)

3.745.1 Informationen

ID	TC_Funktion_IFO_16_686
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.745.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.745.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.745.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_686 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.745.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.746 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_687)

3.746.1 Informationen

ID	TC_Funktion_IFO_16_687
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.746.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.746.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.746.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_687						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.746.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.747 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_688)

3.747.1 Informationen

ID	TC_Funktion_IFO_16_688
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.747.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.747.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.747.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_688 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit

SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.747.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.748 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_689)

3.748.1 Informationen

ID	TC_Funktion_IFO_16_689
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.748.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.748.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.748.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_689						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le

00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.748.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.749 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_690)

3.749.1 Informationen

ID	TC_Funktion_IFO_16_690
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.749.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.749.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.749.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_690						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.749.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.750 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_691)

3.750.1 Informationen

ID	TC_Funktion_IFO_16_691
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase

	'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.750.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.750.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.750.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_691 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.750.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.751 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_692)

3.751.1 Informationen

ID	TC_Funktion_IFO_16_692
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.751.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.751.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.751.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_692 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.751.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.752 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_693)

3.752.1 Informationen

ID	TC_Funktion_IFO_16_693
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.752.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.752.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.752.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_693						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.752.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.753 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_694)

3.753.1 Informationen

ID	TC_Funktion_IFO_16_694
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.753.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.753.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.753.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_694
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.753.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.754 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_695)

3.754.1 Informationen

ID	TC_Funktion_IFO_16_695
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.754.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.754.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.754.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_695						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.754.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.755 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_696)

3.755.1 Informationen

ID	TC_Funktion_IFO_16_696
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.755.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.755.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.755.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_696						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.755.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.756 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_697)

3.756.1 Informationen

ID	TC_Funktion_IFO_16_697
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das

	MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.756.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.756.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.756.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_697						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.756.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.757 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_698)

3.757.1 Informationen

ID	TC_Funktion_IFO_16_698
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.757.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.757.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.757.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_698 GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu

generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'
Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.757.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.758 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_699)

3.758.1 Informationen

ID	TC_Funktion_IFO_16_699
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.758.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.758.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.758.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_699 INTERNAL AUTHENTICATE

CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.758.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.759 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_700)

3.759.1 Informationen

ID	TC_Funktion_IFO_16_700
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.759.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.759.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.759.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_700						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.759.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.760 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_701)

3.760.1 Informationen

ID	TC_Funktion_IFO_16_701
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.760.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.760.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.760.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_701 PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.760.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.761 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_702)

3.761.1 Informationen

ID	TC_Funktion_IFO_16_702
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.761.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.761.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.761.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_702						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.761.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.762 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_703)

3.762.1 Informationen

ID	TC_Funktion_IFO_16_703
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.762.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.762.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.762.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_703 PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.762.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.763 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_704)

3.763.1 Informationen

ID	TC_Funktion_IFO_16_704
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.763.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.763.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.763.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_704						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.763.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.764 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_705)

3.764.1 Informationen

ID	TC_Funktion_IFO_16_705
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.764.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.764.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.764.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_705						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.764.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.765 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_706)

3.765.1 Informationen

ID	TC_Funktion_IFO_16_706
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.765.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.765.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.765.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_706						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.765.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.766 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_707)

3.766.1 Informationen

ID	TC_Funktion_IFO_16_707
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.766.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.766.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.766.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_707						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.766.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.767 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_708)

3.767.1 Informationen

ID	TC_Funktion_IFO_16_708
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.767.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.767.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.767.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_708						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.767.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.768 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_709)

3.768.1 Informationen

ID	TC_Funktion_IFO_16_709
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase

	'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.768.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.768.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.768.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_709						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.768.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.769 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_710)

3.769.1 Informationen

ID	TC_Funktion_IFO_16_710
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.769.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.769.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.769.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_710 ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.769.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.770 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_711)

3.770.1 Informationen

ID	TC_Funktion_IFO_16_711
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.770.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.770.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.770.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_711 ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.770.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.771 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_712)

3.771.1 Informationen

ID	TC_Funktion_IFO_16_712
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.771.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.771.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.771.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_712
ACTIVATE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.771.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.772 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_713)

3.772.1 Informationen

ID	TC_Funktion_IFO_16_713
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.772.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.772.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.772.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_713						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.772.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.773 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_714)

3.773.1 Informationen

ID	TC_Funktion_IFO_16_714
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.773.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.773.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.773.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_714						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.773.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.774 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_715)

3.774.1 Informationen

ID	TC_Funktion_IFO_16_715
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.774.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.774.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.774.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_715						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.774.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.775 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_716)

3.775.1 Informationen

ID	TC_Funktion_IFO_16_716
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die

	Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.775.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.775.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.775.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_716						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.775.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.776 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_717)

3.776.1 Informationen

ID	TC_Funktion_IFO_16_717
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.776.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.776.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.776.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_717 DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.776.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.777 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_718)

3.777.1 Informationen

ID	TC_Funktion_IFO_16_718
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.777.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.777.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.777.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_718						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.777.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.778 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_719)

3.778.1 Informationen

ID	TC_Funktion_IFO_16_719
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.778.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.778.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.778.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_719
DELETE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.778.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.779 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_720)

3.779.1 Informationen

ID	TC_Funktion_IFO_16_720
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.779.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.779.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.779.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_720						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.779.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.780 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_721)

3.780.1 Informationen

ID	TC_Funktion_IFO_16_721
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.780.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.780.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.780.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_721						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.780.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.781 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_722)

3.781.1 Informationen

ID	TC_Funktion_IFO_16_722
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.781.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.781.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.781.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_722						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.781.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.782 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_723)

3.782.1 Informationen

ID	TC_Funktion_IFO_16_723
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.782.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.782.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.782.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_723						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.782.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.783 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_724)

3.783.1 Informationen

ID	TC_Funktion_IFO_16_724
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.783.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.783.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.783.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_724 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit

SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.783.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.784 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_725)

3.784.1 Informationen

ID	TC_Funktion_IFO_16_725
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.784.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.784.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.784.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_725						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le

00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.784.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.785 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_726)

3.785.1 Informationen

ID	TC_Funktion_IFO_16_726
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.785.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.785.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.785.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_726						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.785.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.786 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_727)

3.786.1 Informationen

ID	TC_Funktion_IFO_16_727
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase

	'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.786.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.786.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.786.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_727 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.786.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.787 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_728)

3.787.1 Informationen

ID	TC_Funktion_IFO_16_728
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.787.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.787.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.787.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_728 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.787.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.788 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_729)

3.788.1 Informationen

ID	TC_Funktion_IFO_16_729
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.788.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.788.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.788.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_729						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.788.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.789 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_730)

3.789.1 Informationen

ID	TC_Funktion_IFO_16_730
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.789.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.789.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.789.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_730
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.789.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.790 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_731)

3.790.1 Informationen

ID	TC_Funktion_IFO_16_731
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.790.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.790.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.790.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_731						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.790.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.791 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_732)

3.791.1 Informationen

ID	TC_Funktion_IFO_16_732
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.791.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.791.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.791.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_732						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.791.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.792 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_733)

3.792.1 Informationen

ID	TC_Funktion_IFO_16_733
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das

	MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.792.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.792.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.792.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_733						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.792.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.793 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_734)

3.793.1 Informationen

ID	TC_Funktion_IFO_16_734
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.793.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.793.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.793.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_734 GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu

generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'
Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.793.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.794 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_735)

3.794.1 Informationen

ID	TC_Funktion_IFO_16_735
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.794.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.794.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.794.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_735 INTERNAL AUTHENTICATE

CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.794.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.795 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_736)

3.795.1 Informationen

ID	TC_Funktion_IFO_16_736
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.795.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.795.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.795.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_736						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.795.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.796 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_737)

3.796.1 Informationen

ID	TC_Funktion_IFO_16_737
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.796.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.796.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.796.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_737 PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.796.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.797 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_738)

3.797.1 Informationen

ID	TC_Funktion_IFO_16_738
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.797.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.797.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.797.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_738						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.797.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.798 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_739)

3.798.1 Informationen

ID	TC_Funktion_IFO_16_739
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.798.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.798.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.798.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_739						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.798.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.799 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_740)

3.799.1 Informationen

ID	TC_Funktion_IFO_16_740
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.799.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.799.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.799.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_740 PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.799.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.800 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_741)

3.800.1 Informationen

ID	TC_Funktion_IFO_16_741
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.800.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.800.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.800.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_741 PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.800.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.801 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_742)

3.801.1 Informationen

ID	TC_Funktion_IFO_16_742
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.801.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.801.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.801.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_742						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.801.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.802 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_743)

3.802.1 Informationen

ID	TC_Funktion_IFO_16_743
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.802.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.802.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.802.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_743						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.802.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.803 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_744)

3.803.1 Informationen

ID	TC_Funktion_IFO_16_744
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.803.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.803.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.803.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_744						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.803.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.804 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_745)

3.804.1 Informationen

ID	TC_Funktion_IFO_16_745
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase

	'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_ENC_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.804.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.804.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.804.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_745						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.804.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.805 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_746)

3.805.1 Informationen

ID	TC_Funktion_IFO_16_746
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.805.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.805.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.805.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_746 ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.805.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.806 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_747)

3.806.1 Informationen

ID	TC_Funktion_IFO_16_747
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.806.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.806.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.806.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_747 ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.806.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.807 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_748)

3.807.1 Informationen

ID	TC_Funktion_IFO_16_748
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.807.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.807.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.807.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_748
ACTIVATE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.807.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.808 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_749)

3.808.1 Informationen

ID	TC_Funktion_IFO_16_749
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.808.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.808.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.808.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_749						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.808.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.809 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_750)

3.809.1 Informationen

ID	TC_Funktion_IFO_16_750
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.809.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.809.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.809.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_750						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.809.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.810 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_751)

3.810.1 Informationen

ID	TC_Funktion_IFO_16_751
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.810.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.810.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.810.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_751						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.810.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.811 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_752)

3.811.1 Informationen

ID	TC_Funktion_IFO_16_752
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die

	Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.811.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.811.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.811.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_752						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.811.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.812 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_753)

3.812.1 Informationen

ID	TC_Funktion_IFO_16_753
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.812.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.812.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.812.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_753						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.812.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.813 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_754)

3.813.1 Informationen

ID	TC_Funktion_IFO_16_754
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.813.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.813.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.813.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_754						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.813.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.814 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_755)

3.814.1 Informationen

ID	TC_Funktion_IFO_16_755
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.814.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.814.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.814.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_755
DELETE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.814.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.815 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_756)

3.815.1 Informationen

ID	TC_Funktion_IFO_16_756
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.815.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.815.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.815.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_756						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.815.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.816 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_757)

3.816.1 Informationen

ID	TC_Funktion_IFO_16_757
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.816.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.816.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.816.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_757						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.816.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.817 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_758)

3.817.1 Informationen

ID	TC_Funktion_IFO_16_758
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.817.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.817.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.817.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_758 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.817.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.818 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_759)

3.818.1 Informationen

ID	TC_Funktion_IFO_16_759
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.818.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.818.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.818.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_759 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.818.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.819 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_760)

3.819.1 Informationen

ID	TC_Funktion_IFO_16_760
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.819.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.819.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.819.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_760 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit

SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.819.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.820 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_761)

3.820.1 Informationen

ID	TC_Funktion_IFO_16_761
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.820.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.820.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.820.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_761						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le

00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.820.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.821 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_762)

3.821.1 Informationen

ID	TC_Funktion_IFO_16_762
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.821.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.821.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.821.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_762						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.821.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.822 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_763)

3.822.1 Informationen

ID	TC_Funktion_IFO_16_763
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase

	'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.822.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.822.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.822.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_763 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.822.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.823 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_764)

3.823.1 Informationen

ID	TC_Funktion_IFO_16_764
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.823.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.823.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.823.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_764 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.823.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.824 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_765)

3.824.1 Informationen

ID	TC_Funktion_IFO_16_765
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.824.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.824.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.824.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_765 GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.824.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.825 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_766)

3.825.1 Informationen

ID	TC_Funktion_IFO_16_766
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.825.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.825.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.825.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_766
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.825.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.826 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_767)

3.826.1 Informationen

ID	TC_Funktion_IFO_16_767
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.826.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.826.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.826.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_767						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.826.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.827 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_768)

3.827.1 Informationen

ID	TC_Funktion_IFO_16_768
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.827.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.827.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.827.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_768						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.827.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.828 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_769)

3.828.1 Informationen

ID	TC_Funktion_IFO_16_769
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das

	MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.828.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.828.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.828.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_769						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.828.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.829 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_770)

3.829.1 Informationen

ID	TC_Funktion_IFO_16_770
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.829.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.829.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.829.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_770 GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu

generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'
Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.829.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.830 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_771)

3.830.1 Informationen

ID	TC_Funktion_IFO_16_771
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.830.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.830.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.830.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_771 INTERNAL AUTHENTICATE

CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.830.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.831 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_772)

3.831.1 Informationen

ID	TC_Funktion_IFO_16_772
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.831.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.831.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.831.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_772						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.831.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.832 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_773)

3.832.1 Informationen

ID	TC_Funktion_IFO_16_773
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.832.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.832.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.832.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_773						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.832.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.833 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_774)

3.833.1 Informationen

ID	TC_Funktion_IFO_16_774
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.833.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.833.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.833.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_774						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.833.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.834 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_775)

3.834.1 Informationen

ID	TC_Funktion_IFO_16_775
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.834.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.834.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.834.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_775						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.834.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.835 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_776)

3.835.1 Informationen

ID	TC_Funktion_IFO_16_776
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.835.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.835.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.835.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_776						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.835.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.836 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_777)

3.836.1 Informationen

ID	TC_Funktion_IFO_16_777
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.836.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.836.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.836.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_777						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.836.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.837 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_778)

3.837.1 Informationen

ID	TC_Funktion_IFO_16_778
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.837.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.837.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.837.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_778
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.837.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.838 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_779)

3.838.1 Informationen

ID	TC_Funktion_IFO_16_779
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.838.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.838.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.838.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_779						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.838.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.839 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_780)

3.839.1 Informationen

ID	TC_Funktion_IFO_16_780
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.839.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.839.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.839.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_780						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.839.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.840 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_781)

3.840.1 Informationen

ID	TC_Funktion_IFO_16_781
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.840.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.840.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.840.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_781						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.840.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.841 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_782)

3.841.1 Informationen

ID	TC_Funktion_IFO_16_782
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die

	Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.841.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.841.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.841.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_782						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.841.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.842 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_783)

3.842.1 Informationen

ID	TC_Funktion_IFO_16_783
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.842.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.842.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.842.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_783 ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.842.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.843 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_784)

3.843.1 Informationen

ID	TC_Funktion_IFO_16_784
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.843.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.843.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.843.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_784 CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.843.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.844 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_785)

3.844.1 Informationen

ID	TC_Funktion_IFO_16_785
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.844.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.844.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.844.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_785						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le

00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.844.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.845 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_786)

3.845.1 Informationen

ID	TC_Funktion_IFO_16_786
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.845.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.845.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.845.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_786						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.845.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.846 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_787)

3.846.1 Informationen

ID	TC_Funktion_IFO_16_787
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.846.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.846.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.846.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_787						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.846.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.847 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_788)

3.847.1 Informationen

ID	TC_Funktion_IFO_16_788
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.847.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.847.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.847.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_788						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.847.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.848 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_789)

3.848.1 Informationen

ID	TC_Funktion_IFO_16_789
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die

	Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.848.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.848.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.848.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_789						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.848.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.849 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_790)

3.849.1 Informationen

ID	TC_Funktion_IFO_16_790
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.849.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.849.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.849.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_790 DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.849.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.850 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_791)

3.850.1 Informationen

ID	TC_Funktion_IFO_16_791
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.850.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.850.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.850.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_791 DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.850.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.851 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_792)

3.851.1 Informationen

ID	TC_Funktion_IFO_16_792
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.851.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.851.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.851.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_792
EXTERNAL AUTHENTICATE

CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.851.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.852 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_793)

3.852.1 Informationen

ID	TC_Funktion_IFO_16_793
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.852.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.852.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.852.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_793						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.852.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.853 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_794)

3.853.1 Informationen

ID	TC_Funktion_IFO_16_794
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.853.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.853.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.853.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_794						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.853.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.854 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_795)

3.854.1 Informationen

ID	TC_Funktion_IFO_16_795
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.854.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.854.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.854.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_795						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.854.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.855 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_796)

3.855.1 Informationen

ID	TC_Funktion_IFO_16_796

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.855.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.855.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.855.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_796						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.855.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.856 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_797)

3.856.1 Informationen

ID	TC_Funktion_IFO_16_797
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.856.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.856.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.856.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_797 GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies

im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.856.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.857 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_798)

3.857.1 Informationen

ID	TC_Funktion_IFO_16_798
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.857.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.857.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.857.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_798

GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.857.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.858 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_799)

3.858.1 Informationen

ID	TC_Funktion_IFO_16_799
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.858.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.858.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.858.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_799 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.858.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.859 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_800)

3.859.1 Informationen

ID	TC_Funktion_IFO_16_800
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.859.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.859.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.859.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_800						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.859.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.860 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_801)

3.860.1 Informationen

ID	TC_Funktion_IFO_16_801
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando

	'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.860.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.860.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.860.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_801						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.860.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.861 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_802)

3.861.1 Informationen

ID	TC_Funktion_IFO_16_802
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.861.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.861.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.861.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_802						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.861.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.862 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_803)

3.862.1 Informationen

ID	TC_Funktion_IFO_16_803
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.862.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.862.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.862.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_803						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.862.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.863 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_804)

3.863.1 Informationen

ID	TC_Funktion_IFO_16_804
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.863.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.863.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.863.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_804						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.863.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.864 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_805)

3.864.1 Informationen

ID	TC_Funktion_IFO_16_805
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.864.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.864.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.864.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_805						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.864.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.865 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_806)

3.865.1 Informationen

ID	TC_Funktion_IFO_16_806

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.865.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.865.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.865.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_806						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.865.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.866 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_807)

3.866.1 Informationen

ID	TC_Funktion_IFO_16_807
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.866.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.866.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.866.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_807 INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.866.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.867 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_808)

3.867.1 Informationen

ID	TC_Funktion_IFO_16_808
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.867.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.867.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.867.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_808						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.867.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.868 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_809)

3.868.1 Informationen

ID	TC_Funktion_IFO_16_809
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.868.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.868.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.868.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_809						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.868.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.869 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_810)

3.869.1 Informationen

ID	TC_Funktion_IFO_16_810
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.869.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.869.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.869.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_810						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le

00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.869.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.870 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_811)

3.870.1 Informationen

ID	TC_Funktion_IFO_16_811
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.870.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.870.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.870.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_811						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.870.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.871 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_812)

3.871.1 Informationen

ID	TC_Funktion_IFO_16_812
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.871.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.871.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.871.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_812						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.871.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.872 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_813)

3.872.1 Informationen

ID	TC_Funktion_IFO_16_813
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'PSO

	VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.872.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.872.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.872.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_813						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.872.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.873 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_814)

3.873.1 Informationen

ID	TC_Funktion_IFO_16_814

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.873.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.873.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.873.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_814						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.873.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.874 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_16_815)

3.874.1 Informationen

ID	TC_Funktion_IFO_16_815
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das MF und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.GWA_AUT_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.874.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.874.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.874.4 APDU-Kommandos

ID: CM-Funktion_IFO_16_815						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.874.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.875 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_1)

3.875.1 Informationen

ID	TC_Funktion_IFO_15_1
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.875.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.875.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.875.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_1 ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.875.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.876 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_2)

3.876.1 Informationen

ID	TC_Funktion_IFO_15_2
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'CREATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.876.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.876.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.876.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_2						
CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.876.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.877 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_3)

3.877.1 Informationen

ID	TC_Funktion_IFO_15_3
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'CREATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.877.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.877.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.877.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_3						
CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le

00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.877.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.878 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_4)

3.878.1 Informationen

ID	TC_Funktion_IFO_15_4
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.878.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.878.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.878.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_4

CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.878.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.879 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_5)

3.879.1 Informationen

ID	TC_Funktion_IFO_15_5
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.879.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.879.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.879.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_5						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.879.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.880 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_6)

3.880.1 Informationen

ID	TC_Funktion_IFO_15_6
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.880.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.880.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.880.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_6						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.880.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.881 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_7)

3.881.1 Informationen

ID	TC_Funktion_IFO_15_7
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.881.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.881.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.881.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_7							
DEACTIVATE FILE							
CLA	INS	P1	P2	Lc	Data	Le	
00	04	00	00	--	--	--	

3.881.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.882 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_8)

3.882.1 Informationen

ID	TC_Funktion_IFO_15_8
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'DELETE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.882.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.882.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.882.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_8						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.882.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.883 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_9)

3.883.1 Informationen

ID	TC_Funktion_IFO_15_9
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.883.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.883.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.883.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_9							
DELETE FILE							
CLA	INS	P1	P2	Lc	Data	Le	
00	e4	00	00	--	--	--	

3.883.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.884 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_10)

3.884.1 Informationen

ID	TC_Funktion_IFO_15_10
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'SELECT (DF mittels FID)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.884.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.884.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.884.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_10						
SELECT (DF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden DF.

3.884.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.885 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_11)

3.885.1 Informationen

ID	TC_Funktion_IFO_15_11
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'TERMINATE DF' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.885.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.885.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.885.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_11						
TERMINATE DF						
CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

3.885.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.886 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_12)

3.886.1 Informationen

ID	TC_Funktion_IFO_15_12
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'TERMINATE DF' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.886.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.886.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.886.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_12							
TERMINATE DF							
CLA	INS	P1	P2	Lc	Data	Le	
00	e6	00	00	--	--	--	

3.886.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.887 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_13)

3.887.1 Informationen

ID	TC_Funktion_IFO_15_13
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.887.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.887.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.887.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_13						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.887.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.888 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_14)

3.888.1 Informationen

ID	TC_Funktion_IFO_15_14
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.

Klassifizierung	Gutfall-Test

3.888.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.888.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.888.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_14						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.888.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.889 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_15)

3.889.1 Informationen

ID	TC_Funktion_IFO_15_15
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'DELETE FILE' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.889.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.889.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.889.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_15						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.889.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.890 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_16)

3.890.1 Informationen

ID	TC_Funktion_IFO_15_16
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.

Klassifizierung	Fehlerfall-Test

3.890.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.890.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.890.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_16						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.890.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.891 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_17)

3.891.1 Informationen

ID	TC_Funktion_IFO_15_17
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'READ BINARY (ohne SFI)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je

	nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.891.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.891.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.891.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_17						
READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.891.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.892 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_18)

3.892.1 Informationen

ID	TC_Funktion_IFO_15_18

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'SELECT (DF mittels FID)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.892.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.892.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.892.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_18						
SELECT (DF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden DF.

3.892.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.893 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_19)

3.893.1 Informationen

ID	TC_Funktion_IFO_15_19
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'TERMINATE EF' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.893.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.893.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.893.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_19						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.893.5 Erwartete Ergebnisse

ID	Beschreibung

RS-9000	Das Testsystem antwortet mit '90 00'.

3.894 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_20)

3.894.1 Informationen

ID	TC_Funktion_IFO_15_20
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'UPDATE BINARY (ohne SFI)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.894.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.894.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.894.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_20 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.894.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.895 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_21)

3.895.1 Informationen

ID	TC_Funktion_IFO_15_21
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.895.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.895.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.895.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_21
ACTIVATE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.895.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.896 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_22)

3.896.1 Informationen

ID	TC_Funktion_IFO_15_22
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.896.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.896.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.896.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_22						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.896.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.897 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_23)

3.897.1 Informationen

ID	TC_Funktion_IFO_15_23
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.897.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.897.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.897.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_23						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.897.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.898 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_24)

3.898.1 Informationen

ID	TC_Funktion_IFO_15_24
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.898.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.898.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.898.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_24						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.898.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.899 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_25)

3.899.1 Informationen

ID	TC_Funktion_IFO_15_25
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt

	Key.SMPKIRoot_x, das Kommando 'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.899.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.899.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.899.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_25						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.899.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.900 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_26)

3.900.1 Informationen

ID	TC_Funktion_IFO_15_26
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.900.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.900.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.900.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_26						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.900.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.901 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_27)

3.901.1 Informationen

ID	TC_Funktion_IFO_15_27
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.901.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.901.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.901.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_27 DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.901.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.902 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_28)

3.902.1 Informationen

ID	TC_Funktion_IFO_15_28
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.902.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.902.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.902.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_28

DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.902.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.903 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_29)

3.903.1 Informationen

ID	TC_Funktion_IFO_15_29
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.903.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.903.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.903.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_29 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.903.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.904 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_30)

3.904.1 Informationen

ID	TC_Funktion_IFO_15_30
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.904.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.904.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.904.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_30						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.904.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.905 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_31)

3.905.1 Informationen

ID	TC_Funktion_IFO_15_31
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.905.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.905.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.905.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_31						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.905.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.906 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_32)

3.906.1 Informationen

ID	TC_Funktion_IFO_15_32

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.906.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.906.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.906.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_32						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.906.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.907 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_33)

3.907.1 Informationen

ID	TC_Funktion_IFO_15_33
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.907.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.907.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.907.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_33 GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt

jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.907.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.908 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_34)

3.908.1 Informationen

ID	TC_Funktion_IFO_15_34
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.908.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.908.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.908.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_34						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.908.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.909 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_35)

3.909.1 Informationen

ID	TC_Funktion_IFO_15_35
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.909.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.909.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.909.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_35 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.909.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.910 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_36)

3.910.1 Informationen

ID	TC_Funktion_IFO_15_36
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in

	der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.910.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.910.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.910.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_36 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.910.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.911 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_37)

3.911.1 Informationen

ID	TC_Funktion_IFO_15_37
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.911.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.911.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.911.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_37 GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.911.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.912 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_38)

3.912.1 Informationen

ID	TC_Funktion_IFO_15_38
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.912.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.912.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.912.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_38 GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.912.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.913 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_39)

3.913.1 Informationen

ID	TC_Funktion_IFO_15_39
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.913.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.913.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.913.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_39

GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.913.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.914 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_40)

3.914.1 Informationen

ID	TC_Funktion_IFO_15_40
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.914.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.914.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.914.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_40						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.914.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.915 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_41)

3.915.1 Informationen

ID	TC_Funktion_IFO_15_41
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne

	Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.915.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.915.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.915.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_41						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.915.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.916 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_42)

3.916.1 Informationen

ID	TC_Funktion_IFO_15_42
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.916.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.916.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.916.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_42						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu

generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'
Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.916.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.917 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_43)

3.917.1 Informationen

ID	TC_Funktion_IFO_15_43
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.917.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.917.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.917.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_43 INTERNAL AUTHENTICATE

CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.917.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.918 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_44)

3.918.1 Informationen

ID	TC_Funktion_IFO_15_44
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.918.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.918.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.918.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_44						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.918.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.919 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_45)

3.919.1 Informationen

ID	TC_Funktion_IFO_15_45
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.919.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.919.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.919.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_45						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.919.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.920 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_46)

3.920.1 Informationen

ID	TC_Funktion_IFO_15_46
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.920.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.920.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.920.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_46						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.920.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.921 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_47)

3.921.1 Informationen

ID	TC_Funktion_IFO_15_47
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'PSO VERIFY CERTIFICATE' und

	ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.921.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.921.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.921.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_47 PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.921.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.922 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_48)

3.922.1 Informationen

ID	TC_Funktion_IFO_15_48
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.922.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.922.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.922.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_48						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu

verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.922.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.923 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_49)

3.923.1 Informationen

ID	TC_Funktion_IFO_15_49
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.923.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.923.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.923.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_49

PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.923.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.924 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_50)

3.924.1 Informationen

ID	TC_Funktion_IFO_15_50
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Public-Key-Objekt Key.SMPKIRoot_x, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.924.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.924.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.924.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_50						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.924.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.925 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_51)

3.925.1 Informationen

ID	TC_Funktion_IFO_15_51
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.925.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.925.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.925.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_51 ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.925.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.926 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_52)

3.926.1 Informationen

ID	TC_Funktion_IFO_15_52
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen

	Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.926.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.926.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.926.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_52						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.926.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.927 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_53)

3.927.1 Informationen

ID	TC_Funktion_IFO_15_53
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.927.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.927.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.927.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_53 CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.927.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.928 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_54)

3.928.1 Informationen

ID	TC_Funktion_IFO_15_54
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.928.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.928.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.928.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_54 CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.928.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.929 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_55)

3.929.1 Informationen

ID	TC_Funktion_IFO_15_55
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.929.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.929.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.929.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_55

DEACTIVATE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.929.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.930 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_56)

3.930.1 Informationen

ID	TC_Funktion_IFO_15_56
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.930.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.930.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.930.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_56						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.930.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.931 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_57)

3.931.1 Informationen

ID	TC_Funktion_IFO_15_57
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.931.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.931.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.931.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_57						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.931.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.932 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_58)

3.932.1 Informationen

ID	TC_Funktion_IFO_15_58
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.932.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.932.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.932.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_58						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.932.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.933 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_59)

3.933.1 Informationen

ID	TC_Funktion_IFO_15_59
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und

	GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.933.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.933.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.933.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_59 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.933.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.934 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_60)

3.934.1 Informationen

ID	TC_Funktion_IFO_15_60

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.934.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.934.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.934.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_60						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.934.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.935 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_61)

3.935.1 Informationen

ID	TC_Funktion_IFO_15_61
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.935.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.935.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.935.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_61 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve)

86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.935.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.936 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_62)

3.936.1 Informationen

ID	TC_Funktion_IFO_15_62
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.936.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.936.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.936.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_62
GENERAL AUTHENTICATE (ECKA-DH)

CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.936.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.937 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_63)

3.937.1 Informationen

ID	TC_Funktion_IFO_15_63
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.937.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.937.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.937.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_63						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.937.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.938 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_64)

3.938.1 Informationen

ID	TC_Funktion_IFO_15_64
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in

	der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.938.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.938.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.938.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_64 GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.938.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.939 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_65)

3.939.1 Informationen

ID	TC_Funktion_IFO_15_65
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.939.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.939.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.939.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_65 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.939.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.940 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_66)

3.940.1 Informationen

ID	TC_Funktion_IFO_15_66
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.940.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.940.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.940.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_66 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.940.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.941 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_67)

3.941.1 Informationen

ID	TC_Funktion_IFO_15_67
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.941.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.941.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.941.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_67						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.941.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.942 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_68)

3.942.1 Informationen

ID	TC_Funktion_IFO_15_68
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.942.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.942.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.942.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_68						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.942.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.943 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_69)

3.943.1 Informationen

ID	TC_Funktion_IFO_15_69
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln

	auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.943.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.943.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.943.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_69						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.943.5 Erwartete Ergebnisse

ID	Beschreibung

RS-9000	Das Testsystem antwortet mit '90 00'.

3.944 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_70)

3.944.1 Informationen

ID	TC_Funktion_IFO_15_70
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.944.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.944.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.944.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_70 INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.944.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.945 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_71)

3.945.1 Informationen

ID	TC_Funktion_IFO_15_71
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.945.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.945.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.945.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_71						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.945.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.946 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_72)

3.946.1 Informationen

ID	TC_Funktion_IFO_15_72
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.946.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.946.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.946.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_72

PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.946.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.947 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_73)

3.947.1 Informationen

ID	TC_Funktion_IFO_15_73
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.947.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.947.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.947.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_73						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.947.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.948 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_74)

3.948.1 Informationen

ID	TC_Funktion_IFO_15_74
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.948.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.948.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.948.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_74						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.948.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.949 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_75)

3.949.1 Informationen

ID	TC_Funktion_IFO_15_75
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen

	Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.949.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.949.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.949.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_75						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.949.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.950 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_76)

3.950.1 Informationen

ID	TC_Funktion_IFO_15_76
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.950.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.950.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.950.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_76 PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.950.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.951 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_77)

3.951.1 Informationen

ID	TC_Funktion_IFO_15_77
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.951.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.951.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.951.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_77 PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.951.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.952 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_78)

3.952.1 Informationen

ID	TC_Funktion_IFO_15_78
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_TLS_PRE, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.952.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.952.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.952.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_78						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.952.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.953 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_79)

3.953.1 Informationen

ID	TC_Funktion_IFO_15_79
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.953.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.953.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.953.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_79						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.953.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.954 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_80)

3.954.1 Informationen

ID	TC_Funktion_IFO_15_80
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.954.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.954.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.954.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_80						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.954.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.955 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_81)

3.955.1 Informationen

ID	TC_Funktion_IFO_15_81
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und

	GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.955.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.955.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.955.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_81 CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.955.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.956 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_82)

3.956.1 Informationen

ID	TC_Funktion_IFO_15_82

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.956.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.956.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.956.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_82						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.956.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.957 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_83)

3.957.1 Informationen

ID	TC_Funktion_IFO_15_83
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.957.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.957.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.957.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_83 DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.957.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.958 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_84)

3.958.1 Informationen

ID	TC_Funktion_IFO_15_84
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.958.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.958.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.958.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_84						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.958.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.959 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_85)

3.959.1 Informationen

ID	TC_Funktion_IFO_15_85
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.959.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.959.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.959.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_85 DELETE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.959.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.960 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_86)

3.960.1 Informationen

ID	TC_Funktion_IFO_15_86
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.960.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.960.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.960.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_86						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.960.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.961 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_87)

3.961.1 Informationen

ID	TC_Funktion_IFO_15_87
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.961.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.961.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.961.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_87 EXTERNAL AUTHENTICATE							
CLA	INS	P1	P2	Lc	Data	Le	
00	82	00	00	LL	XX...XX	XX	

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.961.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.962 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_88)

3.962.1 Informationen

ID	TC_Funktion_IFO_15_88
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.962.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.962.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.962.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_88 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.962.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.963 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_89)

3.963.1 Informationen

ID	TC_Funktion_IFO_15_89
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.963.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.963.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.963.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_89						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.963.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.964 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_90)

3.964.1 Informationen

ID	TC_Funktion_IFO_15_90
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.964.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.964.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.964.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_90 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve)

86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.964.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.965 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_91)

3.965.1 Informationen

ID	TC_Funktion_IFO_15_91
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.965.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.965.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.965.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_91
GENERAL AUTHENTICATE (ECKA-EG)

CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.965.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.966 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_92)

3.966.1 Informationen

ID	TC_Funktion_IFO_15_92
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.966.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.966.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.966.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_92						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.966.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.967 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_93)

3.967.1 Informationen

ID	TC_Funktion_IFO_15_93
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in

	der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.967.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.967.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.967.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_93 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.967.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.968 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_94)

3.968.1 Informationen

ID	TC_Funktion_IFO_15_94
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.968.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.968.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.968.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_94 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.968.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.969 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_95)

3.969.1 Informationen

ID	TC_Funktion_IFO_15_95
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.969.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.969.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.969.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_95						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le

00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.969.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.970 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_96)

3.970.1 Informationen

ID	TC_Funktion_IFO_15_96
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.970.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.970.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.970.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_96						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.970.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.971 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_97)

3.971.1 Informationen

ID	TC_Funktion_IFO_15_97
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.971.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.971.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.971.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_97						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.971.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.972 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_98)

3.972.1 Informationen

ID	TC_Funktion_IFO_15_98

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.972.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.972.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.972.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_98						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.972.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.973 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_99)

3.973.1 Informationen

ID	TC_Funktion_IFO_15_99
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.973.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.973.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.973.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_99 INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.973.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.974 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_100)

3.974.1 Informationen

ID	TC_Funktion_IFO_15_100
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.974.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.974.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.974.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_100 PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le

00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.974.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.975 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_101)

3.975.1 Informationen

ID	TC_Funktion_IFO_15_101
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.975.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.975.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.975.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_101						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.975.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.976 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_102)

3.976.1 Informationen

ID	TC_Funktion_IFO_15_102
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.976.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.976.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.976.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_102						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.976.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.977 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_103)

3.977.1 Informationen

ID	TC_Funktion_IFO_15_103
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen

	Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.977.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.977.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.977.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_103						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.977.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.978 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_104)

3.978.1 Informationen

ID	TC_Funktion_IFO_15_104
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.978.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.978.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.978.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_104						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.978.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.979 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_105)

3.979.1 Informationen

ID	TC_Funktion_IFO_15_105
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.979.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.979.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.979.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_105 PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.979.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.980 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_106)

3.980.1 Informationen

ID	TC_Funktion_IFO_15_106
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_SIG_PRE, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.980.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.980.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.980.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_106

PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.980.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.981 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_107)

3.981.1 Informationen

ID	TC_Funktion_IFO_15_107
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.981.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.981.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.981.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_107						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.981.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.982 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_108)

3.982.1 Informationen

ID	TC_Funktion_IFO_15_108
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.982.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.982.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.982.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_108						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.982.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.983 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_109)

3.983.1 Informationen

ID	TC_Funktion_IFO_15_109
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und

	GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.983.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.983.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.983.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_109						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.983.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.984 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_110)

3.984.1 Informationen

ID	TC_Funktion_IFO_15_110
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.984.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.984.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.984.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_110 CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.984.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.985 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_111)

3.985.1 Informationen

ID	TC_Funktion_IFO_15_111
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.985.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.985.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.985.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_111 DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.985.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.986 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_112)

3.986.1 Informationen

ID	TC_Funktion_IFO_15_112
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.986.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.986.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.986.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_112

DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.986.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.987 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_113)

3.987.1 Informationen

ID	TC_Funktion_IFO_15_113
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.987.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.987.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.987.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_113						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.987.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.988 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_114)

3.988.1 Informationen

ID	TC_Funktion_IFO_15_114
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.988.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.988.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.988.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_114						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.988.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.989 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_115)

3.989.1 Informationen

ID	TC_Funktion_IFO_15_115
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und

	GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.989.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.989.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.989.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_115 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.989.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.990 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_116)

3.990.1 Informationen

ID	TC_Funktion_IFO_15_116

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.990.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.990.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.990.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_116						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.990.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.991 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_117)

3.991.1 Informationen

ID	TC_Funktion_IFO_15_117
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.991.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.991.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.991.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_117 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve)

86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.991.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.992 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_118)

3.992.1 Informationen

ID	TC_Funktion_IFO_15_118
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.992.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.992.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.992.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_118 GENERAL AUTHENTICATE (ECKA-DH)

CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.992.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.993 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_119)

3.993.1 Informationen

ID	TC_Funktion_IFO_15_119
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.993.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.993.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.993.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_119						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.993.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.994 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_120)

3.994.1 Informationen

ID	TC_Funktion_IFO_15_120
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in

	der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.994.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.994.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.994.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_120 GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.994.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.995 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_121)

3.995.1 Informationen

ID	TC_Funktion_IFO_15_121
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.995.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.995.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.995.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_121 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.995.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.996 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_122)

3.996.1 Informationen

ID	TC_Funktion_IFO_15_122
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.996.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.996.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.996.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_122 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.996.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.997 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_123)

3.997.1 Informationen

ID	TC_Funktion_IFO_15_123
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.997.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.997.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.997.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_123						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.997.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.998 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_124)

3.998.1 Informationen

ID	TC_Funktion_IFO_15_124
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.998.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.998.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.998.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_124						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.998.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.999 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_125)

3.999.1 Informationen

ID	TC_Funktion_IFO_15_125
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln

	auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.999.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.999.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.999.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_125						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.999.5 Erwartete Ergebnisse

ID	Beschreibung

RS-9000	Das Testsystem antwortet mit '90 00'.

3.1000 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_126)

3.1000.1 Informationen

ID	TC_Funktion_IFO_15_126
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.1000.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1000.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1000.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_126						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1000.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1001 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_127)

3.1001.1 Informationen

ID	TC_Funktion_IFO_15_127
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1001.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1001.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1001.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_127 PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le

00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1001.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1002 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_128)

3.1002.1 Informationen

ID	TC_Funktion_IFO_15_128
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1002.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1002.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1002.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_128						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1002.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1003 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_129)

3.1003.1 Informationen

ID	TC_Funktion_IFO_15_129
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1003.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1003.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1003.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_129						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1003.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1004 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_130)

3.1004.1 Informationen

ID	TC_Funktion_IFO_15_130
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'PSO VERIFY CERTIFICATE'

	und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1004.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1004.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1004.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_130 PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1004.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1005 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_131)

3.1005.1 Informationen

ID	TC_Funktion_IFO_15_131
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1005.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1005.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1005.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_131 PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1005.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1006 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_132)

3.1006.1 Informationen

ID	TC_Funktion_IFO_15_132
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1006.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1006.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1006.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_132 PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1006.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1007 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_133)

3.1007.1 Informationen

ID	TC_Funktion_IFO_15_133
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1007.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1007.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1007.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_133						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1007.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1008 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_134)

3.1008.1 Informationen

ID	TC_Funktion_IFO_15_134
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekt Key.WAN_ENC_PRE, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1008.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1008.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1008.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_134						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1008.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1009 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_135)

3.1009.1 Informationen

ID	TC_Funktion_IFO_15_135
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in

	der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1009.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1009.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1009.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_135						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1009.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1010 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_136)

3.1010.1 Informationen

ID	TC_Funktion_IFO_15_136
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1010.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1010.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1010.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_136 ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1010.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1011 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_137)

3.1011.1 Informationen

ID	TC_Funktion_IFO_15_137
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1011.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1011.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1011.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_137						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1011.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1012 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_138)

3.1012.1 Informationen

ID	TC_Funktion_IFO_15_138
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1012.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1012.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1012.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_138						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le

00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1012.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1013 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_139)

3.1013.1 Informationen

ID	TC_Funktion_IFO_15_139
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1013.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1013.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1013.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_139						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1013.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1014 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_140)

3.1014.1 Informationen

ID	TC_Funktion_IFO_15_140
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1014.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1014.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1014.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_140						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1014.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1015 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_141)

3.1015.1 Informationen

ID	TC_Funktion_IFO_15_141
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1015.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1015.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1015.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_141						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1015.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1016 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_142)

3.1016.1 Informationen

ID	TC_Funktion_IFO_15_142
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und

	GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1016.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1016.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1016.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_142						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1016.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1017 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_143)

3.1017.1 Informationen

ID	TC_Funktion_IFO_15_143
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1017.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1017.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1017.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_143						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1017.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.1018 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_144)

3.1018.1 Informationen

ID	TC_Funktion_IFO_15_144
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1018.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1018.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1018.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_144 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1018.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1019 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_145)

3.1019.1 Informationen

ID	TC_Funktion_IFO_15_145
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1019.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1019.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1019.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_145 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1019.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1020 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_146)

3.1020.1 Informationen

ID	TC_Funktion_IFO_15_146
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1020.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1020.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1020.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_146						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1020.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1021 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_147)

3.1021.1 Informationen

ID	TC_Funktion_IFO_15_147
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1021.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1021.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1021.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_147						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1021.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1022 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_148)

3.1022.1 Informationen

ID	TC_Funktion_IFO_15_148
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1022.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1022.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1022.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_148 GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve

implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1022.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1023 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_149)

3.1023.1 Informationen

ID	TC_Funktion_IFO_15_149
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1023.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1023.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1023.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_149

GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1023.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1024 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_150)

3.1024.1 Informationen

ID	TC_Funktion_IFO_15_150
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1024.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1024.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1024.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_150						
GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1024.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1025 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_151)

3.1025.1 Informationen

ID	TC_Funktion_IFO_15_151
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.1025.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1025.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1025.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_151						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1025.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1026 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_152)

3.1026.1 Informationen

ID	TC_Funktion_IFO_15_152
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen

	Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1026.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1026.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1026.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_152						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1026.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1027 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_153)

3.1027.1 Informationen

ID	TC_Funktion_IFO_15_153
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1027.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1027.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1027.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_153						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template

bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1027.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1028 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_154)

3.1028.1 Informationen

ID	TC_Funktion_IFO_15_154
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1028.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1028.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1028.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_154
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1028.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1029 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_155)

3.1029.1 Informationen

ID	TC_Funktion_IFO_15_155
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1029.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1029.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1029.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_155						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1029.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1030 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_156)

3.1030.1 Informationen

ID	TC_Funktion_IFO_15_156
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und

	GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1030.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1030.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1030.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_156						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1030.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1031 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_157)

3.1031.1 Informationen

ID	TC_Funktion_IFO_15_157
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1031.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1031.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1031.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_157						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1031.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.1032 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_158)

3.1032.1 Informationen

ID	TC_Funktion_IFO_15_158
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1032.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1032.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1032.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_158 INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1032.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1033 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_159)

3.1033.1 Informationen

ID	TC_Funktion_IFO_15_159
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1033.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1033.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1033.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_159 PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1033.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1034 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_160)

3.1034.1 Informationen

ID	TC_Funktion_IFO_15_160
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1034.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1034.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1034.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_160
PSO COMPUTE DIGITAL SIGNATURE

CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1034.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1035 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_161)

3.1035.1 Informationen

ID	TC_Funktion_IFO_15_161
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1035.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1035.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1035.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_161						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1035.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1036 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_162)

3.1036.1 Informationen

ID	TC_Funktion_IFO_15_162
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1036.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1036.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1036.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_162						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1036.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1037 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_163)

3.1037.1 Informationen

ID	TC_Funktion_IFO_15_163
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen

	Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.1037.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1037.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1037.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_163						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1037.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1038 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_164)

3.1038.1 Informationen

ID	TC_Funktion_IFO_15_164
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für Key-Pair-Objekte Key.CA_x, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.1038.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1038.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1038.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_164 PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-

String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1038.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1039 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_165)

3.1039.1 Informationen

ID	TC_Funktion_IFO_15_165
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.1039.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1039.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1039.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_165
ACTIVATE FILE

CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1039.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1040 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_166)

3.1040.1 Informationen

ID	TC_Funktion_IFO_15_166
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1040.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1040.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1040.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_166
DEACTIVATE FILE

CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1040.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1041 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_167)

3.1041.1 Informationen

ID	TC_Funktion_IFO_15_167
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1041.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1041.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1041.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_167

DEACTIVATE FILE

CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1041.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1042 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_168)

3.1042.1 Informationen

ID	TC_Funktion_IFO_15_168
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'DELETE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1042.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1042.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1042.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_168 DELETE FILE

CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1042.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1043 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_169)

3.1043.1 Informationen

ID	TC_Funktion_IFO_15_169
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1043.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1043.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1043.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_169

DELETE FILE

CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1043.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1044 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_170)

3.1044.1 Informationen

ID	TC_Funktion_IFO_15_170
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'READ BINARY (ohne SFI)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.1044.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1044.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1044.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_170

READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1044.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1045 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_171)

3.1045.1 Informationen

ID	TC_Funktion_IFO_15_171
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'SELECT (DF mittels FID)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1045.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1045.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1045.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_171						
SELECT (DF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden DF.

3.1045.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1046 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_172)

3.1046.1 Informationen

ID	TC_Funktion_IFO_15_172
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'TERMINATE EF' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1046.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1046.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1046.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_172						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.1046.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1047 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_173)

3.1047.1 Informationen

ID	TC_Funktion_IFO_15_173
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'TERMINATE EF' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1047.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1047.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1047.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_173						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.1047.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1048 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_174)

3.1048.1 Informationen

ID	TC_Funktion_IFO_15_174
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'UPDATE BINARY (ohne SFI)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist. Dieser Testfall ist nur gültig, sofern der LCSi des EFs auf „initialisation“ steht.
Klassifizierung	Gutfall-Test

3.1048.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1048.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1048.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_174						
UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1048.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1049 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_175)

3.1049.1 Informationen

ID	TC_Funktion_IFO_15_175
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'UPDATE BINARY (ohne SFI)' und ohne Sicherheitszustand. Dieser Testfall ist nur gültig, sofern der LCSi des EFs nicht auf „initialisation“ steht.

Klassifizierung	Gutfall-Test

3.1049.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1049.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1049.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_175 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1049.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1050 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_176)

3.1050.1 Informationen

ID	TC_Funktion_IFO_15_176
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen

	Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'UPDATE BINARY (ohne SFI)' und den Sicherheitszustand PACE. Dieser Testfall ist nur gültig, sofern der LCSi des EFs nicht auf „initialisation“ steht.
Klassifizierung	Gutfall-Test

3.1050.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1050.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1050.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_176 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1050.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1051 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_177)

3.1051.1 Informationen

ID	TC_Funktion_IFO_15_177
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.1051.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1051.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1051.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_177 ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1051.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1052 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_178)

3.1052.1 Informationen

ID	TC_Funktion_IFO_15_178
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1052.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1052.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1052.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_178						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1052.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1053 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_179)

3.1053.1 Informationen

ID	TC_Funktion_IFO_15_179
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1053.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1053.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1053.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_179						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1053.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1054 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_180)

3.1054.1 Informationen

ID	TC_Funktion_IFO_15_180
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'DELETE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1054.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1054.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1054.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_180						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1054.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1055 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_181)

3.1055.1 Informationen

ID	TC_Funktion_IFO_15_181
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1055.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1055.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1055.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_181 DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1055.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1056 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_182)

3.1056.1 Informationen

ID	TC_Funktion_IFO_15_182
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'READ BINARY (ohne SFI)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.1056.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1056.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1056.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_182 READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1056.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1057 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_183)

3.1057.1 Informationen

ID	TC_Funktion_IFO_15_183
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'SELECT (DF mittels FID)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1057.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1057.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1057.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_183 SELECT (DF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden DF.

3.1057.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1058 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_184)

3.1058.1 Informationen

ID	TC_Funktion_IFO_15_184
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'TERMINATE EF' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1058.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1058.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1058.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_184						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.1058.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1059 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_185)

3.1059.1 Informationen

ID	TC_Funktion_IFO_15_185
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'TERMINATE EF' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1059.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1059.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1059.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_185						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.1059.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1060 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_186)

3.1060.1 Informationen

ID	TC_Funktion_IFO_15_186
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'UPDATE BINARY (ohne SFI)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist. Dieser Testfall ist nur gültig, sofern der LCSi des EFs auf „initialisation“ steht.
Klassifizierung	Gutfall-Test

3.1060.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1060.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1060.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_186 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le

00	d6	XX	XX	LL	XX...XX	--

'P1' enthält $(\text{Offset} - P2) / 256$, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1060.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1061 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_187)

3.1061.1 Informationen

ID	TC_Funktion_IFO_15_187
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'UPDATE BINARY (ohne SFI)' und ohne Sicherheitszustand. Dieser Testfall ist nur gültig, sofern der LCSi des EFs nicht auf „initialisation“ steht.
Klassifizierung	Gutfall-Test

3.1061.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1061.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1061.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_187						
UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1061.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1062 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_188)

3.1062.1 Informationen

ID	TC_Funktion_IFO_15_188
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'UPDATE BINARY (ohne SFI)' und den Sicherheitszustand PACE. Dieser Testfall ist nur gültig, sofern der LCSi des EFs nicht auf „initialisation“ steht.
Klassifizierung	Gutfall-Test

3.1062.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1062.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1062.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_188						
UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1062.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1063 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_189)

3.1063.1 Informationen

ID	TC_Funktion_IFO_15_189
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.

Klassifizierung	Gutfall-Test

3.1063.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1063.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1063.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_189						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1063.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1064 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_190)

3.1064.1 Informationen

ID	TC_Funktion_IFO_15_190
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.1064.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1064.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1064.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_190						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1064.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1065 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_191)

3.1065.1 Informationen

ID	TC_Funktion_IFO_15_191
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.

Klassifizierung	Fehlerfall-Test

3.1065.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1065.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1065.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_191 DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1065.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1066 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_192)

3.1066.1 Informationen

ID	TC_Funktion_IFO_15_192
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'DELETE FILE' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.1066.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1066.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1066.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_192						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1066.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1067 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_193)

3.1067.1 Informationen

ID	TC_Funktion_IFO_15_193
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.

Klassifizierung	Fehlerfall-Test

3.1067.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1067.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1067.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_193						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1067.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1068 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_194)

3.1068.1 Informationen

ID	TC_Funktion_IFO_15_194
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'READ BINARY (ohne SFI)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-

	PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.1068.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1068.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1068.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_194 READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1068.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1069 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_195)

3.1069.1 Informationen

ID	TC_Funktion_IFO_15_195
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen

	Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'SELECT (DF mittels FID)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1069.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1069.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1069.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_195 SELECT (DF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden DF.

3.1069.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1070 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_196)

3.1070.1 Informationen

ID	TC_Funktion_IFO_15_196

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'TERMINATE EF' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1070.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1070.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1070.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_196						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.1070.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1071 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_197)

3.1071.1 Informationen

ID	TC_Funktion_IFO_15_197

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'TERMINATE EF' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1071.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1071.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1071.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_197						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.1071.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1072 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_198)

3.1072.1 Informationen

ID	TC_Funktion_IFO_15_198

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'UPDATE BINARY (ohne SFI)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist. Dieser Testfall ist nur gültig, sofern der LCSi des EFs auf „initialisation“ steht.
Klassifizierung	Gutfall-Test

3.1072.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1072.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1072.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_198						
UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1072.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1073 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_199)

3.1073.1 Informationen

ID	TC_Funktion_IFO_15_199
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'UPDATE BINARY (ohne SFI)' und ohne Sicherheitszustand. Dieser Testfall ist nur gültig, sofern der LCSI des EFs nicht auf „initialisation“ steht.
Klassifizierung	Gutfall-Test

3.1073.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1073.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1073.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_199 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1073.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1074 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_200)

3.1074.1 Informationen

ID	TC_Funktion_IFO_15_200
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'UPDATE BINARY (ohne SFI)' und den Sicherheitszustand PACE. Dieser Testfall ist nur gültig, sofern der LCSi des EFs nicht auf „initialisation“ steht.
Klassifizierung	Gutfall-Test

3.1074.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1074.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1074.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_200 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1074.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1075 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_201)

3.1075.1 Informationen

ID	TC_Funktion_IFO_15_201
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GWKeys (Datenfeld für symmetrische GW-Keys), das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.1075.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1075.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1075.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_201							
ACTIVATE FILE							
CLA	INS	P1	P2	Lc	Data	Le	
00	44	00	00	--	--	--	

3.1075.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1076 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_202)

3.1076.1 Informationen

ID	TC_Funktion_IFO_15_202
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GWKeys (Datenfeld für symmetrische GW-Keys), das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.1076.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1076.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1076.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_202 DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1076.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1077 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_203)

3.1077.1 Informationen

ID	TC_Funktion_IFO_15_203
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GWKeys (Datenfeld für symmetrische GW-Keys), das Kommando 'DELETE FILE' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.1077.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1077.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1077.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_203						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1077.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1078 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_204)

3.1078.1 Informationen

ID	TC_Funktion_IFO_15_204
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GWKeys (Datenfeld für symmetrische GW-Keys), das Kommando 'READ RECORD (ohne SFI)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.1078.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1078.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1078.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_204						
READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1078.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1079 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_205)

3.1079.1 Informationen

ID	TC_Funktion_IFO_15_205
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GWKeys (Datenfeld für symmetrische GW-Keys), das Kommando 'SELECT (DF mittels FID)' und ohne Sicherheitszustand.

Klassifizierung	Gutfall-Test

3.1079.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1079.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1079.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_205 SELECT (DF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden DF.

3.1079.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1080 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_206)

3.1080.1 Informationen

ID	TC_Funktion_IFO_15_206
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GWKeys (Datenfeld für

	symmetrische GW-Keys), das Kommando 'TERMINATE EF' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.1080.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1080.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1080.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_206						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.1080.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1081 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_15_207)

3.1081.1 Informationen

ID	TC_Funktion_IFO_15_207
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln

	auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Vor-Personalisierung + Integration von Sicherheitsmodul und GW'. Die Durchführung erfolgt für EF.GWKeys (Datenfeld für symmetrische GW-Keys), das Kommando 'UPDATE RECORD (ohne SFI)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.1081.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1081.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1081.4 APDU-Kommandos

ID: CM-Funktion_IFO_15_207						
UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1081.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1082 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_208)

3.1082.1 Informationen

ID	TC_Funktion_IFO_17_208
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'ACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1082.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1082.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1082.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_208						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1082.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1083 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_209)

3.1083.1 Informationen

ID	TC_Funktion_IFO_17_209
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1083.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1083.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1083.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_209						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1083.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1084 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_210)

3.1084.1 Informationen

ID	TC_Funktion_IFO_17_210
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1084.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1084.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1084.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_210						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1084.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1085 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_211)

3.1085.1 Informationen

ID	TC_Funktion_IFO_17_211
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'CREATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1085.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1085.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1085.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_211 CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1085.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.1086 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_212)

3.1086.1 Informationen

ID	TC_Funktion_IFO_17_212
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'CREATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1086.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1086.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1086.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_212 CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1086.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1087 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_213)

3.1087.1 Informationen

ID	TC_Funktion_IFO_17_213
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'CREATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1087.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1087.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1087.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_213						
CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1087.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1088 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_214)

3.1088.1 Informationen

ID	TC_Funktion_IFO_17_214
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1088.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1088.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1088.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_214 CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le

00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1088.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1089 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_215)

3.1089.1 Informationen

ID	TC_Funktion_IFO_17_215
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1089.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1089.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1089.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_215						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1089.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1090 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_216)

3.1090.1 Informationen

ID	TC_Funktion_IFO_17_216
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1090.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1090.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1090.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_216						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1090.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1091 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_217)

3.1091.1 Informationen

ID	TC_Funktion_IFO_17_217
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1091.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1091.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1091.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_217 DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1091.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1092 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_218)

3.1092.1 Informationen

ID	TC_Funktion_IFO_17_218
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1092.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1092.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1092.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_218 DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1092.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1093 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_219)

3.1093.1 Informationen

ID	TC_Funktion_IFO_17_219
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1093.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1093.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1093.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_219 DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1093.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1094 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_220)

3.1094.1 Informationen

ID	TC_Funktion_IFO_17_220
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'DELETE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1094.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1094.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1094.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_220						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1094.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1095 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_221)

3.1095.1 Informationen

ID	TC_Funktion_IFO_17_221
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1095.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1095.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1095.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_221						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1095.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1096 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_222)

3.1096.1 Informationen

ID	TC_Funktion_IFO_17_222
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'SELECT (DF mittels FID)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1096.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1096.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1096.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_222						
SELECT (DF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	XX XX	--

'Data' enthält den File-Identifizierer des zu selektierenden DF.

3.1096.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1097 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_223)

3.1097.1 Informationen

ID	TC_Funktion_IFO_17_223
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'TERMINATE DF' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1097.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1097.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1097.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_223						
TERMINATE DF						
CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

3.1097.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1098 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_224)

3.1098.1 Informationen

ID	TC_Funktion_IFO_17_224
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'TERMINATE DF' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1098.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1098.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1098.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_224						
TERMINATE DF						
CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

3.1098.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1099 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_225)

3.1099.1 Informationen

ID	TC_Funktion_IFO_17_225
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für DF.SMGW, das Kommando 'TERMINATE DF' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1099.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1099.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1099.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_225						
TERMINATE DF						
CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

3.1099.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1100 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_226)

3.1100.1 Informationen

ID	TC_Funktion_IFO_17_226
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'ACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1100.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1100.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1100.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_226						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1100.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1101 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_227)

3.1101.1 Informationen

ID	TC_Funktion_IFO_17_227
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1101.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1101.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1101.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_227						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1101.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1102 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_228)

3.1102.1 Informationen

ID	TC_Funktion_IFO_17_228
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1102.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1102.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1102.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_228						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1102.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1103 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_229)

3.1103.1 Informationen

ID	TC_Funktion_IFO_17_229
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'CREATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1103.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1103.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1103.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_229						
CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1103.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1104 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_230)

3.1104.1 Informationen

ID	TC_Funktion_IFO_17_230
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW angelegte DFs und deren weitere über CREATE FILE angelegte

	Unterordner, das Kommando 'CREATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1104.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1104.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1104.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_230						
CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1104.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1105 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_231)

3.1105.1 Informationen

ID	TC_Funktion_IFO_17_231

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'CREATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1105.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1105.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1105.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_231						
CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1105.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1106 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_232)

3.1106.1 Informationen

ID	TC_Funktion_IFO_17_232
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1106.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1106.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1106.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_232						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1106.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1107 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_233)

3.1107.1 Informationen

ID	TC_Funktion_IFO_17_233
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1107.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1107.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1107.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_233 CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1107.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1108 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_234)

3.1108.1 Informationen

ID	TC_Funktion_IFO_17_234
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1108.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1108.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1108.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_234						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1108.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1109 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_235)

3.1109.1 Informationen

ID	TC_Funktion_IFO_17_235
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1109.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1109.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1109.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_235							
DEACTIVATE FILE							
CLA	INS	P1	P2	Lc	Data	Le	
00	04	00	00	--	--	--	

3.1109.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1110 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_236)

3.1110.1 Informationen

ID	TC_Funktion_IFO_17_236
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1110.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1110.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1110.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_236							
DEACTIVATE FILE							
CLA	INS	P1	P2	Lc	Data	Le	
00	04	00	00	--	--	--	

3.1110.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1111 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_237)

3.1111.1 Informationen

ID	TC_Funktion_IFO_17_237
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1111.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1111.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1111.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_237							
DEACTIVATE FILE							
CLA	INS	P1	P2	Lc	Data	Le	
00	04	00	00	--	--	--	

3.1111.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1112 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_238)

3.1112.1 Informationen

ID	TC_Funktion_IFO_17_238
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'DELETE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1112.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1112.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1112.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_238						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1112.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1113 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_239)

3.1113.1 Informationen

ID	TC_Funktion_IFO_17_239
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1113.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1113.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1113.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_239						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1113.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1114 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_240)

3.1114.1 Informationen

ID	TC_Funktion_IFO_17_240
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'DELETE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1114.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1114.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1114.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_240						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1114.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1115 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_241)

3.1115.1 Informationen

ID	TC_Funktion_IFO_17_241
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'SELECT (DF mittels FID)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1115.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1115.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1115.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_241 SELECT (DF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden DF.

3.1115.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1116 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_242)

3.1116.1 Informationen

ID	TC_Funktion_IFO_17_242
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'TERMINATE DF' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1116.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1116.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1116.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_242						
TERMINATE DF						
CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

3.1116.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1117 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_243)

3.1117.1 Informationen

ID	TC_Funktion_IFO_17_243
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'TERMINATE DF' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1117.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1117.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1117.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_243						
TERMINATE DF						
CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

3.1117.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1118 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_244)

3.1118.1 Informationen

ID	TC_Funktion_IFO_17_244
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW angelegte DFs und deren weitere über CREATE FILE angelegte Unterordner, das Kommando 'TERMINATE DF' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1118.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1118.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1118.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_244						
TERMINATE DF						
CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

3.1118.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1119 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_245)

3.1119.1 Informationen

ID	TC_Funktion_IFO_17_245
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des DF.SMGW angelegte EFs, das Kommando 'ACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1119.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1119.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1119.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_245						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1119.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1120 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_246)

3.1120.1 Informationen

ID	TC_Funktion_IFO_17_246
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des DF.SMGW angelegte EFs, das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1120.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1120.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1120.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_246						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1120.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1121 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_247)

3.1121.1 Informationen

ID	TC_Funktion_IFO_17_247
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des DF.SMGW angelegte EFs, das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1121.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1121.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1121.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_247						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1121.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1122 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_248)

3.1122.1 Informationen

ID	TC_Funktion_IFO_17_248
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des DF.SMGW angelegte EFs, das Kommando 'APPEND RECORD (ohne SFI)' und ohne Sicherheitszustand. Dieser Testfall ist nur gültig, sofern das Kommando im Sicherheitsmodul implementiert ist

Klassifizierung	Fehlerfall-Test

3.1122.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1122.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1122.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_248 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1122.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1123 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_249)

3.1123.1 Informationen

ID	TC_Funktion_IFO_17_249
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die

	Durchführung erfolgt für über CREATE FILE im DF.SMGW und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des DF.SMGW angelegte EFs, das Kommando 'APPEND RECORD (ohne SFI)' und den Sicherheitszustand PACE. Dieser Testfall ist nur gültig, sofern das Kommando im Sicherheitsmodul implementiert ist
Klassifizierung	Fehlerfall-Test

3.1123.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1123.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1123.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_249 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1123.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1124 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_250)

3.1124.1 Informationen

ID	TC_Funktion_IFO_17_250
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des DF.SMGW angelegte EFs, das Kommando 'APPEND RECORD (ohne SFI)' und den Sicherheitszustand PACE + AUTH. Dieser Testfall ist nur gültig, sofern das Kommando im Sicherheitsmodul implementiert ist
Klassifizierung	Gutfall-Test

3.1124.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1124.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1124.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_250 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1124.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1125 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_251)

3.1125.1 Informationen

ID	TC_Funktion_IFO_17_251
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des DF.SMGW angelegte EFs, das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1125.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1125.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1125.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_251 DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1125.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1126 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_252)

3.1126.1 Informationen

ID	TC_Funktion_IFO_17_252
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des DF.SMGW angelegte EFs, das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1126.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1126.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1126.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_252 DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1126.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1127 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_253)

3.1127.1 Informationen

ID	TC_Funktion_IFO_17_253
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des DF.SMGW angelegte EFs, das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1127.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1127.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1127.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_253 DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1127.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1128 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_254)

3.1128.1 Informationen

ID	TC_Funktion_IFO_17_254
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des DF.SMGW angelegte EFs, das Kommando 'DELETE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1128.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1128.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1128.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_254 DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1128.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1129 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_255)

3.1129.1 Informationen

ID	TC_Funktion_IFO_17_255
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des DF.SMGW angelegte EFs, das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1129.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1129.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1129.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_255 DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1129.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1130 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_256)

3.1130.1 Informationen

ID	TC_Funktion_IFO_17_256
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des DF.SMGW angelegte EFs, das Kommando 'DELETE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1130.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1130.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1130.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_256 DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1130.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1131 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_257)

3.1131.1 Informationen

ID	TC_Funktion_IFO_17_257
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des DF.SMGW angelegte EFs, das Kommando 'SELECT (DF mittels FID)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1131.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1131.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1131.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_257 SELECT (DF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden DF.

3.1131.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1132 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_258)

3.1132.1 Informationen

ID	TC_Funktion_IFO_17_258
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des DF.SMGW angelegte EFs, das Kommando 'TERMINATE EF' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1132.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1132.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1132.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_258							
TERMINATE EF							
CLA	INS	P1	P2	Lc	Data	Le	

00	e8	00	00	--	--	--

3.1132.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1133 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_259)

3.1133.1 Informationen

ID	TC_Funktion_IFO_17_259
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des DF.SMGW angelegte EFs, das Kommando 'TERMINATE EF' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1133.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1133.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1133.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_259
TERMINATE EF

CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.1133.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1134 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_260)

3.1134.1 Informationen

ID	TC_Funktion_IFO_17_260
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des DF.SMGW angelegte EFs, das Kommando 'TERMINATE EF' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1134.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1134.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1134.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_260

TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.1134.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1135 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_261)

3.1135.1 Informationen

ID	TC_Funktion_IFO_17_261
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des DF.SMGW angelegte EFs, das Kommando 'READ BINARY (ohne SFI) / READ RECORD (ohne SFI)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1135.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1135.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1135.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_261						
READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

ID: CM-Funktion_IFO_17_261						
READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1135.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1136 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_262)

3.1136.1 Informationen

ID	TC_Funktion_IFO_17_262
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des DF.SMGW angelegte EFs, das Kommando 'READ BINARY (ohne SFI) /

	READ RECORD (ohne SFI)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1136.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1136.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1136.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_262 READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

ID: CM-Funktion_IFO_17_262 READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1136.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1137 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_263)

3.1137.1 Informationen

ID	TC_Funktion_IFO_17_263
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des DF.SMGW angelegte EFs, das Kommando 'READ BINARY (ohne SFI) / READ RECORD (ohne SFI)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1137.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1137.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1137.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_263 READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

ID: CM-Funktion_IFO_17_263

READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1137.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1138 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_264)

3.1138.1 Informationen

ID	TC_Funktion_IFO_17_264
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des DF.SMGW angelegte EFs, das Kommando 'UPDATE BINARY (ohne SFI) / UPDATE RECORD (ohne SFI)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1138.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1138.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1138.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_264						
UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

ID: CM-Funktion_IFO_17_264						
UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1138.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1139 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_265)

3.1139.1 Informationen

ID	TC_Funktion_IFO_17_265
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die

	Durchführung erfolgt für über CREATE FILE im DF.SMGW und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des DF.SMGW angelegte EFs, das Kommando 'UPDATE BINARY (ohne SFI) / UPDATE RECORD (ohne SFI)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1139.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1139.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1139.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_265 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

ID: CM-Funktion_IFO_17_265 UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1139.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1140 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_266)

3.1140.1 Informationen

ID	TC_Funktion_IFO_17_266
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für über CREATE FILE im DF.SMGW und in weiteren ebenfalls über CREATE FILE angelegten Unterordnern des DF.SMGW angelegte EFs, das Kommando 'UPDATE BINARY (ohne SFI) / UPDATE RECORD (ohne SFI)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1140.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1140.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1140.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_266 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le

00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

ID: CM-Funktion_IFO_17_266 UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1140.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1141 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_267)

3.1141.1 Informationen

ID	TC_Funktion_IFO_17_267
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'ACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1141.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1141.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1141.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_267						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1141.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1142 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_268)

3.1142.1 Informationen

ID	TC_Funktion_IFO_17_268
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1142.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1142.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1142.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_268						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1142.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1143 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_269)

3.1143.1 Informationen

ID	TC_Funktion_IFO_17_269
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1143.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1143.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1143.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_269						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1143.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1144 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_270)

3.1144.1 Informationen

ID	TC_Funktion_IFO_17_270
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1144.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1144.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1144.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_270						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1144.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1145 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_271)

3.1145.1 Informationen

ID	TC_Funktion_IFO_17_271
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1145.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1145.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1145.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_271						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1145.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1146 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_272)

3.1146.1 Informationen

ID	TC_Funktion_IFO_17_272
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1146.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1146.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1146.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_272						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1146.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1147 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_273)

3.1147.1 Informationen

ID	TC_Funktion_IFO_17_273
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'DELETE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1147.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1147.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1147.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_273						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1147.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1148 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_274)

3.1148.1 Informationen

ID	TC_Funktion_IFO_17_274
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1148.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1148.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1148.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_274						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1148.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1149 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_275)

3.1149.1 Informationen

ID	TC_Funktion_IFO_17_275
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'DELETE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1149.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1149.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1149.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_275						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1149.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1150 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_276)

3.1150.1 Informationen

ID	TC_Funktion_IFO_17_276
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'READ BINARY (ohne SFI)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1150.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1150.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1150.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_276						
READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1150.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1151 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_277)

3.1151.1 Informationen

ID	TC_Funktion_IFO_17_277
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'READ BINARY (ohne SFI)' und den

	Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1151.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1151.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1151.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_277 READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1151.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1152 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_278)

3.1152.1 Informationen

ID	TC_Funktion_IFO_17_278
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen

	Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'SELECT (DF mittels FID)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1152.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1152.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1152.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_278						
SELECT (DF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden DF.

3.1152.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1153 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_279)

3.1153.1 Informationen

ID	TC_Funktion_IFO_17_279
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'TERMINATE EF' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1153.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1153.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1153.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_279						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.1153.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1154 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_280)

3.1154.1 Informationen

ID	TC_Funktion_IFO_17_280
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'TERMINATE EF' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1154.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1154.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1154.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_280						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.1154.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1155 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_281)

3.1155.1 Informationen

ID	TC_Funktion_IFO_17_281
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'TERMINATE EF' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1155.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1155.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1155.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_281						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.1155.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1156 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_282)

3.1156.1 Informationen

ID	TC_Funktion_IFO_17_282
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'UPDATE BINARY (ohne SFI)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1156.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1156.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1156.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_282 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1156.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1157 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_283)

3.1157.1 Informationen

ID	TC_Funktion_IFO_17_283
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'UPDATE BINARY (ohne SFI)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1157.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1157.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1157.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_283 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1157.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1158 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_284)

3.1158.1 Informationen

ID	TC_Funktion_IFO_17_284
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.SMPKIRoot_x (Datenfelder für SM-PKI-Root-Zertifikate), das Kommando 'UPDATE BINARY (ohne SFI)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1158.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1158.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1158.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_284 UPDATE BINARY (ohne SFI)

CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1158.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1159 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_285)

3.1159.1 Informationen

ID	TC_Funktion_IFO_17_285
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'ACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1159.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1159.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1159.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_285							
ACTIVATE FILE							
CLA	INS	P1	P2	Lc	Data	Le	
00	44	00	00	--	--	--	

3.1159.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1160 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_286)

3.1160.1 Informationen

ID	TC_Funktion_IFO_17_286
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1160.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1160.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1160.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_286							
ACTIVATE FILE							
CLA	INS	P1	P2	Lc	Data	Le	
00	44	00	00	--	--	--	

3.1160.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1161 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_287)

3.1161.1 Informationen

ID	TC_Funktion_IFO_17_287
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1161.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1161.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1161.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_287						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1161.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1162 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_288)

3.1162.1 Informationen

ID	TC_Funktion_IFO_17_288
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1162.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1162.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1162.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_288							
DEACTIVATE FILE							
CLA	INS	P1	P2	Lc	Data	Le	
00	04	00	00	--	--	--	

3.1162.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1163 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_289)

3.1163.1 Informationen

ID	TC_Funktion_IFO_17_289
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'DELETE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1163.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1163.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1163.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_289						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1163.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1164 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_290)

3.1164.1 Informationen

ID	TC_Funktion_IFO_17_290
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1164.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1164.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1164.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_290							
DELETE FILE							
CLA	INS	P1	P2	Lc	Data	Le	
00	e4	00	00	--	--	--	

3.1164.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1165 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_291)

3.1165.1 Informationen

ID	TC_Funktion_IFO_17_291
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'READ BINARY (ohne SFI)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1165.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1165.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1165.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_291						
READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1165.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1166 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_292)

3.1166.1 Informationen

ID	TC_Funktion_IFO_17_292
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'READ BINARY (ohne SFI)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1166.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1166.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1166.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_292						
READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1166.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1167 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_293)

3.1167.1 Informationen

ID	TC_Funktion_IFO_17_293
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'SELECT (DF mittels FID)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1167.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1167.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1167.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_293						
SELECT (DF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	XX XX	--

'Data' enthält den File-Identifizierer des zu selektierenden DF.

3.1167.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1168 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_294)

3.1168.1 Informationen

ID	TC_Funktion_IFO_17_294
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'TERMINATE EF' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1168.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1168.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1168.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_294						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.1168.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1169 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_295)

3.1169.1 Informationen

ID	TC_Funktion_IFO_17_295
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'TERMINATE EF' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1169.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1169.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1169.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_295						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.1169.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1170 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_296)

3.1170.1 Informationen

ID	TC_Funktion_IFO_17_296
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'UPDATE BINARY (ohne SFI)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1170.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1170.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1170.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_296 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1170.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1171 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_297)

3.1171.1 Informationen

ID	TC_Funktion_IFO_17_297
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die

	Durchführung erfolgt für EF.GSCert_TLS, das Kommando 'UPDATE BINARY (ohne SFI)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1171.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1171.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1171.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_297						
UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1171.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1172 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_298)

3.1172.1 Informationen

ID	TC_Funktion_IFO_17_298
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'ACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1172.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1172.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1172.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_298							
ACTIVATE FILE							
CLA	INS	P1	P2	Lc	Data	Le	
00	44	00	00	--	--	--	

3.1172.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1173 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_299)

3.1173.1 Informationen

ID	TC_Funktion_IFO_17_299
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1173.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1173.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1173.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_299						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1173.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1174 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_300)

3.1174.1 Informationen

ID	TC_Funktion_IFO_17_300
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1174.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1174.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1174.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_300 DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1174.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1175 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_301)

3.1175.1 Informationen

ID	TC_Funktion_IFO_17_301
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1175.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1175.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1175.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_301 DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1175.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1176 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_302)

3.1176.1 Informationen

ID	TC_Funktion_IFO_17_302
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'DELETE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1176.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1176.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1176.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_302						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1176.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1177 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_303)

3.1177.1 Informationen

ID	TC_Funktion_IFO_17_303
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1177.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1177.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1177.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_303						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1177.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1178 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_304)

3.1178.1 Informationen

ID	TC_Funktion_IFO_17_304
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'READ BINARY (ohne SFI)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1178.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1178.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1178.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_304 READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1178.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.1179 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_305)

3.1179.1 Informationen

ID	TC_Funktion_IFO_17_305
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'READ BINARY (ohne SFI)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1179.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1179.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1179.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_305 READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1179.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1180 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_306)

3.1180.1 Informationen

ID	TC_Funktion_IFO_17_306
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'SELECT (DF mittels FID)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1180.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1180.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1180.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_306 SELECT (DF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden DF.

3.1180.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1181 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_307)

3.1181.1 Informationen

ID	TC_Funktion_IFO_17_307
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'TERMINATE EF' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1181.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1181.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1181.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_307						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.1181.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1182 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_308)

3.1182.1 Informationen

ID	TC_Funktion_IFO_17_308
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'TERMINATE EF' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1182.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1182.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1182.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_308						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.1182.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1183 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_309)

3.1183.1 Informationen

ID	TC_Funktion_IFO_17_309
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'UPDATE BINARY (ohne SFI)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1183.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1183.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1183.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_309 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1183.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1184 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_310)

3.1184.1 Informationen

ID	TC_Funktion_IFO_17_310
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_SIG, das Kommando 'UPDATE BINARY (ohne SFI)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1184.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1184.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1184.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_310 UPDATE BINARY (ohne SFI)

CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1184.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1185 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_311)

3.1185.1 Informationen

ID	TC_Funktion_IFO_17_311
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'ACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1185.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1185.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1185.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_311							
ACTIVATE FILE							
CLA	INS	P1	P2	Lc	Data	Le	
00	44	00	00	--	--	--	

3.1185.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1186 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_312)

3.1186.1 Informationen

ID	TC_Funktion_IFO_17_312
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1186.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1186.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1186.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_312							
ACTIVATE FILE							
CLA	INS	P1	P2	Lc	Data	Le	
00	44	00	00	--	--	--	

3.1186.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1187 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_313)

3.1187.1 Informationen

ID	TC_Funktion_IFO_17_313
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1187.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1187.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1187.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_313							
DEACTIVATE FILE							
CLA	INS	P1	P2	Lc	Data	Le	
00	04	00	00	--	--	--	

3.1187.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1188 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_314)

3.1188.1 Informationen

ID	TC_Funktion_IFO_17_314
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1188.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1188.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1188.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_314							
DEACTIVATE FILE							
CLA	INS	P1	P2	Lc	Data	Le	
00	04	00	00	--	--	--	

3.1188.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1189 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_315)

3.1189.1 Informationen

ID	TC_Funktion_IFO_17_315
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'DELETE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1189.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1189.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1189.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_315						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1189.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1190 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_316)

3.1190.1 Informationen

ID	TC_Funktion_IFO_17_316
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1190.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1190.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1190.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_316							
DELETE FILE							
CLA	INS	P1	P2	Lc	Data	Le	
00	e4	00	00	--	--	--	

3.1190.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1191 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_317)

3.1191.1 Informationen

ID	TC_Funktion_IFO_17_317
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'READ BINARY (ohne SFI)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1191.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1191.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1191.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_317						
READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1191.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1192 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_318)

3.1192.1 Informationen

ID	TC_Funktion_IFO_17_318
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'READ BINARY (ohne SFI)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1192.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1192.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1192.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_318						
READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1192.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1193 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_319)

3.1193.1 Informationen

ID	TC_Funktion_IFO_17_319
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'SELECT (DF mittels FID)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1193.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1193.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1193.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_319 SELECT (DF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	XX XX	--

'Data' enthält den File-Identifizierer des zu selektierenden DF.

3.1193.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1194 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_320)

3.1194.1 Informationen

ID	TC_Funktion_IFO_17_320
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'TERMINATE EF' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1194.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1194.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1194.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_320						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.1194.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1195 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_321)

3.1195.1 Informationen

ID	TC_Funktion_IFO_17_321
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'TERMINATE EF' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1195.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1195.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1195.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_321						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.1195.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1196 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_322)

3.1196.1 Informationen

ID	TC_Funktion_IFO_17_322
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'UPDATE BINARY (ohne SFI)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1196.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1196.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1196.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_322						
UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1196.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1197 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_323)

3.1197.1 Informationen

ID	TC_Funktion_IFO_17_323
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die

	Durchführung erfolgt für EF.GSCert_ENC, das Kommando 'UPDATE BINARY (ohne SFI)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1197.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1197.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1197.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_323						
UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1197.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1198 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_324)

3.1198.1 Informationen

ID	TC_Funktion_IFO_17_324
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GWKeys (Datenfeld für symmetrische GW-Keys), das Kommando 'ACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1198.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1198.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1198.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_324						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1198.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1199 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_325)

3.1199.1 Informationen

ID	TC_Funktion_IFO_17_325
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GWKeys (Datenfeld für symmetrische GW-Keys), das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1199.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1199.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1199.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_325						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1199.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1200 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_326)

3.1200.1 Informationen

ID	TC_Funktion_IFO_17_326
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GWKeys (Datenfeld für symmetrische GW-Keys), das Kommando 'APPEND RECORD (ohne SFI)' und ohne Sicherheitszustand. Dieser Testfall ist nur gültig, sofern das Kommando im Sicherheitsmodul implementiert ist
Klassifizierung	Fehlerfall-Test

3.1200.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1200.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1200.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_326 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1200.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1201 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_327)

3.1201.1 Informationen

ID	TC_Funktion_IFO_17_327
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GWKeys (Datenfeld für symmetrische GW-Keys), das Kommando 'APPEND RECORD (ohne SFI)' und den Sicherheitszustand PACE. Dieser Testfall ist nur gültig, sofern das Kommando im Sicherheitsmodul implementiert ist
Klassifizierung	Fehlerfall-Test

3.1201.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1201.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1201.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_327 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1201.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1202 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_328)

3.1202.1 Informationen

ID	TC_Funktion_IFO_17_328
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GWKeys (Datenfeld für symmetrische GW-Keys), das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1202.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1202.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1202.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_328 DEACTIVATE FILE

CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1202.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1203 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_329)

3.1203.1 Informationen

ID	TC_Funktion_IFO_17_329
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GWKeys (Datenfeld für symmetrische GW-Keys), das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1203.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1203.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1203.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_329
DEACTIVATE FILE

CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1203.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1204 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_330)

3.1204.1 Informationen

ID	TC_Funktion_IFO_17_330
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GWKeys (Datenfeld für symmetrische GW-Keys), das Kommando 'DELETE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1204.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1204.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1204.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_330
DELETE FILE

CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1204.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1205 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_331)

3.1205.1 Informationen

ID	TC_Funktion_IFO_17_331
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GWKeys (Datenfeld für symmetrische GW-Keys), das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1205.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1205.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1205.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_331

DELETE FILE

CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1205.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1206 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_332)

3.1206.1 Informationen

ID	TC_Funktion_IFO_17_332
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GWKeys (Datenfeld für symmetrische GW-Keys), das Kommando 'READ RECORD (ohne SFI)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1206.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1206.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1206.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_332 READ RECORD (ohne SFI)

CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1206.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1207 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_333)

3.1207.1 Informationen

ID	TC_Funktion_IFO_17_333
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GWKeys (Datenfeld für symmetrische GW-Keys), das Kommando 'READ RECORD (ohne SFI)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1207.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1207.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1207.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_333						
READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1207.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1208 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_334)

3.1208.1 Informationen

ID	TC_Funktion_IFO_17_334
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GWKeys (Datenfeld für symmetrische GW-Keys), das Kommando 'SELECT (DF mittels FID)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1208.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1208.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1208.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_334 SELECT (DF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden DF.

3.1208.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1209 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_335)

3.1209.1 Informationen

ID	TC_Funktion_IFO_17_335
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GWKeys (Datenfeld für symmetrische GW-Keys), das Kommando 'TERMINATE EF' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1209.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1209.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1209.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_335						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.1209.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1210 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_336)

3.1210.1 Informationen

ID	TC_Funktion_IFO_17_336
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GWKeys (Datenfeld für symmetrische GW-Keys), das Kommando 'TERMINATE EF' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1210.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1210.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1210.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_336						
TERMINATE EF						
CLA	INS	P1	P2	Lc	Data	Le
00	e8	00	00	--	--	--

3.1210.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1211 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_337)

3.1211.1 Informationen

ID	TC_Funktion_IFO_17_337
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GWKeys (Datenfeld für symmetrische GW-Keys), das Kommando 'UPDATE RECORD (ohne SFI)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1211.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1211.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1211.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_337 UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1211.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1212 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_338)

3.1212.1 Informationen

ID	TC_Funktion_IFO_17_338
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das MF und die initialen Dateien und Objekte im MF in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für EF.GWKeys (Datenfeld für symmetrische GW-Keys), das Kommando 'UPDATE RECORD (ohne SFI)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1212.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1212.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1212.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_338 UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1212.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1213 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_339)

3.1213.1 Informationen

ID	TC_Funktion_IFO_17_339
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1213.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1213.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1213.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_339						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1213.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1214 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_340)

3.1214.1 Informationen

ID	TC_Funktion_IFO_17_340
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'.

	Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1214.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1214.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1214.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_340						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1214.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1215 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_341)

3.1215.1 Informationen

ID	TC_Funktion_IFO_17_341
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1215.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1215.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1215.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_341 ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1215.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1216 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_342)

3.1216.1 Informationen

ID	TC_Funktion_IFO_17_342
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1216.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1216.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1216.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_342						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1216.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1217 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_343)

3.1217.1 Informationen

ID	TC_Funktion_IFO_17_343
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1217.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1217.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1217.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_343						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le

00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1217.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1218 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_344)

3.1218.1 Informationen

ID	TC_Funktion_IFO_17_344
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1218.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1218.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1218.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_344						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1218.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1219 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_345)

3.1219.1 Informationen

ID	TC_Funktion_IFO_17_345
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1219.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1219.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1219.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_345						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1219.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1220 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_346)

3.1220.1 Informationen

ID	TC_Funktion_IFO_17_346
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1220.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1220.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1220.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_346						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1220.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1221 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_347)

3.1221.1 Informationen

ID	TC_Funktion_IFO_17_347
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'.

	Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1221.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1221.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1221.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_347						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1221.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1222 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_348)

3.1222.1 Informationen

ID	TC_Funktion_IFO_17_348
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1222.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1222.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1222.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_348 DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1222.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1223 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_349)

3.1223.1 Informationen

ID	TC_Funktion_IFO_17_349
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1223.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1223.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1223.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_349						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1223.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1224 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_350)

3.1224.1 Informationen

ID	TC_Funktion_IFO_17_350
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1224.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1224.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1224.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_350 EXTERNAL AUTHENTICATE

CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1224.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1225 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_351)

3.1225.1 Informationen

ID	TC_Funktion_IFO_17_351
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1225.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1225.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1225.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_351 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1225.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1226 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_352)

3.1226.1 Informationen

ID	TC_Funktion_IFO_17_352
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1226.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1226.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1226.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_352						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1226.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1227 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_353)

3.1227.1 Informationen

ID	TC_Funktion_IFO_17_353
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.

Klassifizierung	Fehlerfall-Test

3.1227.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1227.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1227.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_353						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1227.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1228 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_354)

3.1228.1 Informationen

ID	TC_Funktion_IFO_17_354
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1228.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1228.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1228.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_354 GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator

sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1228.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1229 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_355)

3.1229.1 Informationen

ID	TC_Funktion_IFO_17_355
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1229.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1229.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1229.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_355 GENERAL AUTHENTICATE (ECKA-EG)

CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1229.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1230 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_356)

3.1230.1 Informationen

ID	TC_Funktion_IFO_17_356
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1230.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1230.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1230.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_356						
GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1230.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1231 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_357)

3.1231.1 Informationen

ID	TC_Funktion_IFO_17_357
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.

Klassifizierung	Fehlerfall-Test

3.1231.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1231.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1231.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_357						
GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1231.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1232 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_358)

3.1232.1 Informationen

ID	TC_Funktion_IFO_17_358

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1232.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1232.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1232.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_358						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1232.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1233 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_359)

3.1233.1 Informationen

ID	TC_Funktion_IFO_17_359
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1233.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1233.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1233.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_359						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1233.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1234 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_360)

3.1234.1 Informationen

ID	TC_Funktion_IFO_17_360
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1234.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1234.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1234.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_360						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1234.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1235 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_361)

3.1235.1 Informationen

ID	TC_Funktion_IFO_17_361
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1235.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1235.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1235.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_361						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1235.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1236 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_362)

3.1236.1 Informationen

ID	TC_Funktion_IFO_17_362
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1236.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1236.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1236.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_362						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1236.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1237 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_363)

3.1237.1 Informationen

ID	TC_Funktion_IFO_17_363

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1237.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1237.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1237.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_363						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1237.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.1238 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_364)

3.1238.1 Informationen

ID	TC_Funktion_IFO_17_364
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1238.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1238.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1238.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_364 INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1238.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1239 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_365)

3.1239.1 Informationen

ID	TC_Funktion_IFO_17_365
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1239.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1239.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1239.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_365						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1239.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1240 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_366)

3.1240.1 Informationen

ID	TC_Funktion_IFO_17_366
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1240.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1240.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1240.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_366						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le

00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1240.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1241 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_367)

3.1241.1 Informationen

ID	TC_Funktion_IFO_17_367
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1241.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1241.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1241.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_367

PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1241.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1242 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_368)

3.1242.1 Informationen

ID	TC_Funktion_IFO_17_368
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1242.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1242.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1242.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_368						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1242.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1243 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_369)

3.1243.1 Informationen

ID	TC_Funktion_IFO_17_369
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1243.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1243.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1243.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_369						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1243.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1244 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_370)

3.1244.1 Informationen

ID	TC_Funktion_IFO_17_370
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen

	Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1244.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1244.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1244.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_370						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1244.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1245 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_371)

3.1245.1 Informationen

ID	TC_Funktion_IFO_17_371
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1245.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1245.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1245.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_371 PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1245.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1246 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_372)

3.1246.1 Informationen

ID	TC_Funktion_IFO_17_372
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'activated')' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.1246.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1246.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1246.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_372 PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'activated')						
CLA	INS	P1	P2	Lc	Data	Le

00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1246.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1247 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_373)

3.1247.1 Informationen

ID	TC_Funktion_IFO_17_373
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'deactivated')' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1247.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1247.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1247.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_373 PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'deactivated')						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1247.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1248 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_374)

3.1248.1 Informationen

ID	TC_Funktion_IFO_17_374
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'deactivated')' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1248.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1248.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1248.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_374 PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'deactivated')						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1248.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1249 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_375)

3.1249.1 Informationen

ID	TC_Funktion_IFO_17_375
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln

	auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'initialisation')' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1249.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1249.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1249.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_375 PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'initialisation')						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1249.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1250 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_376)

3.1250.1 Informationen

ID	TC_Funktion_IFO_17_376
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.SMPKIRoot_x, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'initialisation')' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1250.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1250.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1250.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_376 PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key im operational state 'initialisation')						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1250.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1251 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_377)

3.1251.1 Informationen

ID	TC_Funktion_IFO_17_377
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1251.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1251.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1251.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_377						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1251.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1252 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_378)

3.1252.1 Informationen

ID	TC_Funktion_IFO_17_378
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1252.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1252.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1252.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_378
ACTIVATE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1252.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1253 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_379)

3.1253.1 Informationen

ID	TC_Funktion_IFO_17_379
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1253.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1253.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1253.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_379						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1253.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1254 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_380)

3.1254.1 Informationen

ID	TC_Funktion_IFO_17_380
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1254.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1254.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1254.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_380						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1254.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1255 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_381)

3.1255.1 Informationen

ID	TC_Funktion_IFO_17_381
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1255.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1255.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1255.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_381						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1255.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1256 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_382)

3.1256.1 Informationen

ID	TC_Funktion_IFO_17_382
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'.

	Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1256.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1256.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1256.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_382						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1256.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1257 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_383)

3.1257.1 Informationen

ID	TC_Funktion_IFO_17_383
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1257.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1257.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1257.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_383 DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1257.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1258 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_384)

3.1258.1 Informationen

ID	TC_Funktion_IFO_17_384
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1258.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1258.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1258.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_384 DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1258.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1259 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_385)

3.1259.1 Informationen

ID	TC_Funktion_IFO_17_385
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1259.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1259.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1259.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_385
EXTERNAL AUTHENTICATE

CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1259.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1260 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_386)

3.1260.1 Informationen

ID	TC_Funktion_IFO_17_386
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1260.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1260.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1260.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_386						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1260.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1261 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_387)

3.1261.1 Informationen

ID	TC_Funktion_IFO_17_387
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1261.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1261.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1261.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_387						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1261.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1262 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_388)

3.1262.1 Informationen

ID	TC_Funktion_IFO_17_388
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.

Klassifizierung	Fehlerfall-Test

3.1262.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1262.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1262.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_388						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1262.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1263 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_389)

3.1263.1 Informationen

ID	TC_Funktion_IFO_17_389
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1263.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1263.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1263.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_389 GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator

sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1263.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1264 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_390)

3.1264.1 Informationen

ID	TC_Funktion_IFO_17_390
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1264.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1264.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1264.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_390
GENERAL AUTHENTICATE (ECKA-EG)

CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1264.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1265 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_391)

3.1265.1 Informationen

ID	TC_Funktion_IFO_17_391
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1265.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1265.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1265.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_391						
GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1265.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1266 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_392)

3.1266.1 Informationen

ID	TC_Funktion_IFO_17_392
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.

Klassifizierung	Fehlerfall-Test

3.1266.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1266.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1266.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_392						
GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1266.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1267 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_393)

3.1267.1 Informationen

ID	TC_Funktion_IFO_17_393

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1267.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1267.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1267.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_393						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1267.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1268 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_394)

3.1268.1 Informationen

ID	TC_Funktion_IFO_17_394
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1268.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1268.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1268.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_394 GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1268.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1269 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_395)

3.1269.1 Informationen

ID	TC_Funktion_IFO_17_395
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1269.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1269.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1269.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_395						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1269.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1270 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_396)

3.1270.1 Informationen

ID	TC_Funktion_IFO_17_396
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1270.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1270.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1270.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_396						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1270.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1271 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_397)

3.1271.1 Informationen

ID	TC_Funktion_IFO_17_397
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1271.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1271.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1271.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_397						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1271.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1272 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_398)

3.1272.1 Informationen

ID	TC_Funktion_IFO_17_398

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1272.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1272.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1272.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_398						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1272.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.1273 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_399)

3.1273.1 Informationen

ID	TC_Funktion_IFO_17_399
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1273.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1273.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1273.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_399 INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1273.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1274 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_400)

3.1274.1 Informationen

ID	TC_Funktion_IFO_17_400
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1274.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1274.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1274.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_400						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1274.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1275 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_401)

3.1275.1 Informationen

ID	TC_Funktion_IFO_17_401
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1275.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1275.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1275.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_401							
PSO COMPUTE DIGITAL SIGNATURE							
CLA	INS	P1	P2	Lc	Data	Le	

00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1275.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1276 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_402)

3.1276.1 Informationen

ID	TC_Funktion_IFO_17_402
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1276.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1276.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1276.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_402

PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1276.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1277 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_403)

3.1277.1 Informationen

ID	TC_Funktion_IFO_17_403
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1277.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1277.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1277.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_403						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1277.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1278 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_404)

3.1278.1 Informationen

ID	TC_Funktion_IFO_17_404
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1278.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1278.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1278.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_404						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1278.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1279 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_405)

3.1279.1 Informationen

ID	TC_Funktion_IFO_17_405
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen

	Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1279.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1279.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1279.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_405						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1279.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1280 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_406)

3.1280.1 Informationen

ID	TC_Funktion_IFO_17_406
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1280.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1280.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1280.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_406						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1280.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1281 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_407)

3.1281.1 Informationen

ID	TC_Funktion_IFO_17_407
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1281.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1281.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1281.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_407 PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1281.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1282 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_408)

3.1282.1 Informationen

ID	TC_Funktion_IFO_17_408
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS_PRE, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1282.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1282.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1282.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_408

PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1282.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1283 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_409)

3.1283.1 Informationen

ID	TC_Funktion_IFO_17_409
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1283.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1283.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1283.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_409						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1283.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1284 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_410)

3.1284.1 Informationen

ID	TC_Funktion_IFO_17_410
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1284.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1284.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1284.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_410						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1284.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1285 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_411)

3.1285.1 Informationen

ID	TC_Funktion_IFO_17_411
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1285.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1285.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1285.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_411						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1285.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1286 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_412)

3.1286.1 Informationen

ID	TC_Funktion_IFO_17_412
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando

	'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1286.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1286.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1286.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_412						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1286.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1287 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_413)

3.1287.1 Informationen

ID	TC_Funktion_IFO_17_413

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1287.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1287.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1287.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_413						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1287.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1288 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_414)

3.1288.1 Informationen

ID	TC_Funktion_IFO_17_414
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1288.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1288.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1288.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_414 DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1288.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1289 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_415)

3.1289.1 Informationen

ID	TC_Funktion_IFO_17_415
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1289.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1289.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1289.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_415						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1289.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1290 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_416)

3.1290.1 Informationen

ID	TC_Funktion_IFO_17_416
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1290.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1290.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1290.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_416
DELETE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1290.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1291 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_417)

3.1291.1 Informationen

ID	TC_Funktion_IFO_17_417
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1291.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1291.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1291.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_417 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1291.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1292 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_418)

3.1292.1 Informationen

ID	TC_Funktion_IFO_17_418
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1292.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1292.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1292.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_418 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1292.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1293 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_419)

3.1293.1 Informationen

ID	TC_Funktion_IFO_17_419
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1293.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1293.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1293.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_419						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1293.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1294 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_420)

3.1294.1 Informationen

ID	TC_Funktion_IFO_17_420
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'.

	Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1294.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1294.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1294.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_420 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1294.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1295 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_421)

3.1295.1 Informationen

ID	TC_Funktion_IFO_17_421
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1295.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1295.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1295.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_421 GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator

sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1295.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1296 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_422)

3.1296.1 Informationen

ID	TC_Funktion_IFO_17_422
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1296.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1296.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1296.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_422
GENERAL AUTHENTICATE (ECKA-EG)

CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1296.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1297 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_423)

3.1297.1 Informationen

ID	TC_Funktion_IFO_17_423
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1297.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1297.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1297.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_423 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1297.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1298 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_424)

3.1298.1 Informationen

ID	TC_Funktion_IFO_17_424
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.

Klassifizierung	Fehlerfall-Test

3.1298.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1298.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1298.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_424						
GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1298.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1299 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_425)

3.1299.1 Informationen

ID	TC_Funktion_IFO_17_425

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1299.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1299.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1299.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_425						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1299.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1300 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_426)

3.1300.1 Informationen

ID	TC_Funktion_IFO_17_426
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1300.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1300.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1300.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_426						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1300.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1301 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_427)

3.1301.1 Informationen

ID	TC_Funktion_IFO_17_427
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1301.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1301.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1301.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_427						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1301.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1302 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_428)

3.1302.1 Informationen

ID	TC_Funktion_IFO_17_428
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1302.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1302.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1302.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_428						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1302.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1303 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_429)

3.1303.1 Informationen

ID	TC_Funktion_IFO_17_429
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1303.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1303.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1303.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_429						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1303.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1304 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_430)

3.1304.1 Informationen

ID	TC_Funktion_IFO_17_430

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1304.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1304.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1304.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_430						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1304.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.1305 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_431)

3.1305.1 Informationen

ID	TC_Funktion_IFO_17_431
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1305.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1305.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1305.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_431 INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1305.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1306 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_432)

3.1306.1 Informationen

ID	TC_Funktion_IFO_17_432
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1306.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1306.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1306.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_432						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1306.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1307 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_433)

3.1307.1 Informationen

ID	TC_Funktion_IFO_17_433
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1307.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1307.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1307.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_433							
PSO COMPUTE DIGITAL SIGNATURE							
CLA	INS	P1	P2	Lc	Data	Le	

00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1307.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1308 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_434)

3.1308.1 Informationen

ID	TC_Funktion_IFO_17_434
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1308.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1308.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1308.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_434

PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1308.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1309 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_435)

3.1309.1 Informationen

ID	TC_Funktion_IFO_17_435
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1309.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1309.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1309.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_435						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1309.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1310 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_436)

3.1310.1 Informationen

ID	TC_Funktion_IFO_17_436
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1310.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1310.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1310.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_436						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1310.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1311 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_437)

3.1311.1 Informationen

ID	TC_Funktion_IFO_17_437
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen

	Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1311.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1311.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1311.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_437						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1311.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1312 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_438)

3.1312.1 Informationen

ID	TC_Funktion_IFO_17_438
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1312.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1312.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1312.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_438						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1312.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1313 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_439)

3.1313.1 Informationen

ID	TC_Funktion_IFO_17_439
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1313.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1313.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1313.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_439						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1313.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1314 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_440)

3.1314.1 Informationen

ID	TC_Funktion_IFO_17_440
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG_PRE, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1314.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1314.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1314.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_440

PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1314.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1315 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_441)

3.1315.1 Informationen

ID	TC_Funktion_IFO_17_441
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1315.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1315.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1315.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_441 ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1315.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1316 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_442)

3.1316.1 Informationen

ID	TC_Funktion_IFO_17_442
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1316.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1316.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1316.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_442						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1316.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1317 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_443)

3.1317.1 Informationen

ID	TC_Funktion_IFO_17_443
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1317.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1317.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1317.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_443						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1317.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1318 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_444)

3.1318.1 Informationen

ID	TC_Funktion_IFO_17_444
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando

	'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1318.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1318.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1318.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_444						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1318.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1319 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_445)

3.1319.1 Informationen

ID	TC_Funktion_IFO_17_445

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1319.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1319.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1319.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_445						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1319.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1320 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_446)

3.1320.1 Informationen

ID	TC_Funktion_IFO_17_446
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1320.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1320.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1320.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_446 DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1320.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1321 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_447)

3.1321.1 Informationen

ID	TC_Funktion_IFO_17_447
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1321.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1321.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1321.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_447						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1321.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1322 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_448)

3.1322.1 Informationen

ID	TC_Funktion_IFO_17_448
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1322.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1322.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1322.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_448
DELETE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1322.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1323 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_449)

3.1323.1 Informationen

ID	TC_Funktion_IFO_17_449
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1323.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1323.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1323.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_449 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1323.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1324 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_450)

3.1324.1 Informationen

ID	TC_Funktion_IFO_17_450
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1324.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1324.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1324.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_450 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1324.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1325 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_451)

3.1325.1 Informationen

ID	TC_Funktion_IFO_17_451
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1325.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1325.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1325.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_451						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1325.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1326 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_452)

3.1326.1 Informationen

ID	TC_Funktion_IFO_17_452
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'.

	Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1326.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1326.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1326.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_452 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1326.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1327 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_453)

3.1327.1 Informationen

ID	TC_Funktion_IFO_17_453
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1327.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1327.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1327.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_453 GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator

sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1327.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1328 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_454)

3.1328.1 Informationen

ID	TC_Funktion_IFO_17_454
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1328.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1328.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1328.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_454
GENERAL AUTHENTICATE (ECKA-EG)

CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1328.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1329 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_455)

3.1329.1 Informationen

ID	TC_Funktion_IFO_17_455
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1329.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1329.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1329.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_455						
GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1329.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1330 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_456)

3.1330.1 Informationen

ID	TC_Funktion_IFO_17_456
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.

Klassifizierung	Fehlerfall-Test

3.1330.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1330.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1330.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_456						
GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1330.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1331 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_457)

3.1331.1 Informationen

ID	TC_Funktion_IFO_17_457

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1331.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1331.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1331.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_457						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1331.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1332 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_458)

3.1332.1 Informationen

ID	TC_Funktion_IFO_17_458
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1332.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1332.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1332.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_458						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1332.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1333 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_459)

3.1333.1 Informationen

ID	TC_Funktion_IFO_17_459
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1333.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1333.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1333.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_459						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1333.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1334 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_460)

3.1334.1 Informationen

ID	TC_Funktion_IFO_17_460
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1334.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1334.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1334.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_460						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1334.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1335 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_461)

3.1335.1 Informationen

ID	TC_Funktion_IFO_17_461
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1335.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1335.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1335.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_461						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1335.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1336 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_462)

3.1336.1 Informationen

ID	TC_Funktion_IFO_17_462

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1336.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1336.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1336.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_462						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1336.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.1337 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_463)

3.1337.1 Informationen

ID	TC_Funktion_IFO_17_463
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1337.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1337.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1337.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_463 INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1337.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1338 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_464)

3.1338.1 Informationen

ID	TC_Funktion_IFO_17_464
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1338.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1338.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1338.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_464						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1338.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1339 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_465)

3.1339.1 Informationen

ID	TC_Funktion_IFO_17_465
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1339.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1339.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1339.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_465							
PSO COMPUTE DIGITAL SIGNATURE							
CLA	INS	P1	P2	Lc	Data	Le	

00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1339.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1340 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_466)

3.1340.1 Informationen

ID	TC_Funktion_IFO_17_466
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1340.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1340.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1340.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_466

PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1340.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1341 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_467)

3.1341.1 Informationen

ID	TC_Funktion_IFO_17_467
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1341.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1341.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1341.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_467						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1341.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1342 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_468)

3.1342.1 Informationen

ID	TC_Funktion_IFO_17_468
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1342.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1342.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1342.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_468						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1342.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1343 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_469)

3.1343.1 Informationen

ID	TC_Funktion_IFO_17_469
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen

	Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1343.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1343.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1343.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_469						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1343.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1344 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_470)

3.1344.1 Informationen

ID	TC_Funktion_IFO_17_470
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1344.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1344.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1344.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_470 PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1344.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1345 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_471)

3.1345.1 Informationen

ID	TC_Funktion_IFO_17_471
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1345.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1345.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1345.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_471 PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1345.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1346 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_472)

3.1346.1 Informationen

ID	TC_Funktion_IFO_17_472
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC_PRE, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1346.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1346.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1346.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_472

PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1346.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1347 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_473)

3.1347.1 Informationen

ID	TC_Funktion_IFO_17_473
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1347.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1347.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1347.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_473						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1347.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1348 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_474)

3.1348.1 Informationen

ID	TC_Funktion_IFO_17_474
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1348.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1348.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1348.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_474						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1348.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1349 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_475)

3.1349.1 Informationen

ID	TC_Funktion_IFO_17_475
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1349.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1349.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1349.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_475						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1349.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1350 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_476)

3.1350.1 Informationen

ID	TC_Funktion_IFO_17_476
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'.

	Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1350.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1350.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1350.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_476						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1350.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1351 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_477)

3.1351.1 Informationen

ID	TC_Funktion_IFO_17_477

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1351.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1351.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1351.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_477						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1351.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1352 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_478)

3.1352.1 Informationen

ID	TC_Funktion_IFO_17_478
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1352.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1352.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1352.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_478 DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1352.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1353 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_479)

3.1353.1 Informationen

ID	TC_Funktion_IFO_17_479
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1353.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1353.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1353.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_479						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1353.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1354 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_480)

3.1354.1 Informationen

ID	TC_Funktion_IFO_17_480
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1354.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1354.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1354.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_480
DEACTIVATE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1354.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1355 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_481)

3.1355.1 Informationen

ID	TC_Funktion_IFO_17_481
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1355.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1355.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1355.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_481						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1355.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1356 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_482)

3.1356.1 Informationen

ID	TC_Funktion_IFO_17_482
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1356.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1356.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1356.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_482						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1356.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1357 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_483)

3.1357.1 Informationen

ID	TC_Funktion_IFO_17_483
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1357.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1357.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1357.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_483						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1357.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1358 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_484)

3.1358.1 Informationen

ID	TC_Funktion_IFO_17_484
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'.

	Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1358.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1358.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1358.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_484 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1358.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1359 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_485)

3.1359.1 Informationen

ID	TC_Funktion_IFO_17_485
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen

	Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1359.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1359.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1359.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_485 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1359.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1360 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_486)

3.1360.1 Informationen

ID	TC_Funktion_IFO_17_486
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1360.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1360.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1360.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_486 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve)

86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1360.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1361 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_487)

3.1361.1 Informationen

ID	TC_Funktion_IFO_17_487
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1361.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1361.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1361.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_487
GENERAL AUTHENTICATE (ECKA-DH)

CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1361.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1362 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_488)

3.1362.1 Informationen

ID	TC_Funktion_IFO_17_488
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1362.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1362.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1362.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_488						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1362.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1363 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_489)

3.1363.1 Informationen

ID	TC_Funktion_IFO_17_489
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in

	der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1363.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1363.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1363.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_489 GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1363.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1364 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_490)

3.1364.1 Informationen

ID	TC_Funktion_IFO_17_490
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1364.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1364.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1364.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_490 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1364.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1365 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_491)

3.1365.1 Informationen

ID	TC_Funktion_IFO_17_491
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1365.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1365.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1365.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_491 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1365.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1366 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_492)

3.1366.1 Informationen

ID	TC_Funktion_IFO_17_492
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1366.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1366.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1366.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_492						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1366.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1367 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_493)

3.1367.1 Informationen

ID	TC_Funktion_IFO_17_493
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1367.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1367.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1367.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_493						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1367.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1368 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_494)

3.1368.1 Informationen

ID	TC_Funktion_IFO_17_494
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1368.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1368.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1368.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_494						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1368.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1369 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_495)

3.1369.1 Informationen

ID	TC_Funktion_IFO_17_495
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln

	auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1369.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1369.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1369.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_495						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1369.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1370 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_496)

3.1370.1 Informationen

ID	TC_Funktion_IFO_17_496
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1370.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1370.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1370.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_496						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1370.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1371 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_497)

3.1371.1 Informationen

ID	TC_Funktion_IFO_17_497
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1371.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1371.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1371.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_497						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1371.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1372 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_498)

3.1372.1 Informationen

ID	TC_Funktion_IFO_17_498
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1372.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1372.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1372.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_498						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1372.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1373 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_499)

3.1373.1 Informationen

ID	TC_Funktion_IFO_17_499
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1373.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1373.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1373.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_499						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1373.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1374 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_500)

3.1374.1 Informationen

ID	TC_Funktion_IFO_17_500

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1374.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1374.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1374.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_500						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1374.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1375 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_501)

3.1375.1 Informationen

ID	TC_Funktion_IFO_17_501
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1375.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1375.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1375.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_501 INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1375.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.1376 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_502)

3.1376.1 Informationen

ID	TC_Funktion_IFO_17_502
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1376.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1376.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1376.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_502 PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1376.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1377 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_503)

3.1377.1 Informationen

ID	TC_Funktion_IFO_17_503
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1377.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1377.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1377.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_503						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1377.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1378 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_504)

3.1378.1 Informationen

ID	TC_Funktion_IFO_17_504
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1378.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1378.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1378.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_504						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le

00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1378.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1379 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_505)

3.1379.1 Informationen

ID	TC_Funktion_IFO_17_505
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1379.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1379.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1379.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_505						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1379.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1380 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_506)

3.1380.1 Informationen

ID	TC_Funktion_IFO_17_506
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1380.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1380.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1380.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_506						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1380.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1381 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_507)

3.1381.1 Informationen

ID	TC_Funktion_IFO_17_507
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'PSO

	VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1381.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1381.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1381.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_507						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1381.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1382 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_508)

3.1382.1 Informationen

ID	TC_Funktion_IFO_17_508

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1382.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1382.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1382.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_508						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1382.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1383 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_509)

3.1383.1 Informationen

ID	TC_Funktion_IFO_17_509
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_TLS, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1383.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1383.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1383.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_509						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1383.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1384 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_510)

3.1384.1 Informationen

ID	TC_Funktion_IFO_17_510
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1384.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1384.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1384.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_510 ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1384.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1385 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_511)

3.1385.1 Informationen

ID	TC_Funktion_IFO_17_511
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1385.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1385.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1385.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_511
ACTIVATE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1385.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1386 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_512)

3.1386.1 Informationen

ID	TC_Funktion_IFO_17_512
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1386.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1386.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1386.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_512						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1386.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1387 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_513)

3.1387.1 Informationen

ID	TC_Funktion_IFO_17_513
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1387.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1387.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1387.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_513						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1387.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1388 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_514)

3.1388.1 Informationen

ID	TC_Funktion_IFO_17_514
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1388.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1388.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1388.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_514						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1388.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1389 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_515)

3.1389.1 Informationen

ID	TC_Funktion_IFO_17_515
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando

	'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1389.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1389.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1389.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_515						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1389.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1390 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_516)

3.1390.1 Informationen

ID	TC_Funktion_IFO_17_516

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1390.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1390.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1390.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_516						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1390.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1391 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_517)

3.1391.1 Informationen

ID	TC_Funktion_IFO_17_517
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1391.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1391.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1391.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_517 DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1391.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1392 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_518)

3.1392.1 Informationen

ID	TC_Funktion_IFO_17_518
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1392.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1392.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1392.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_518						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1392.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1393 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_519)

3.1393.1 Informationen

ID	TC_Funktion_IFO_17_519
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1393.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1393.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1393.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_519
DELETE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1393.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1394 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_520)

3.1394.1 Informationen

ID	TC_Funktion_IFO_17_520
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1394.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1394.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1394.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_520						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1394.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1395 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_521)

3.1395.1 Informationen

ID	TC_Funktion_IFO_17_521
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1395.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1395.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1395.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_521 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1395.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1396 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_522)

3.1396.1 Informationen

ID	TC_Funktion_IFO_17_522
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1396.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1396.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1396.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_522						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1396.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1397 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_523)

3.1397.1 Informationen

ID	TC_Funktion_IFO_17_523
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.1397.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1397.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1397.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_523						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1397.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1398 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_524)

3.1398.1 Informationen

ID	TC_Funktion_IFO_17_524
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1398.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1398.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1398.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_524 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve)

86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1398.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1399 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_525)

3.1399.1 Informationen

ID	TC_Funktion_IFO_17_525
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1399.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1399.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1399.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_525						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le

00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1399.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1400 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_526)

3.1400.1 Informationen

ID	TC_Funktion_IFO_17_526
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1400.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1400.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1400.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_526						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1400.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1401 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_527)

3.1401.1 Informationen

ID	TC_Funktion_IFO_17_527
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in

	der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1401.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1401.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1401.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_527						
GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1401.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1402 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_528)

3.1402.1 Informationen

ID	TC_Funktion_IFO_17_528
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1402.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1402.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1402.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_528 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1402.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1403 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_529)

3.1403.1 Informationen

ID	TC_Funktion_IFO_17_529
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1403.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1403.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1403.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_529						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1403.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1404 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_530)

3.1404.1 Informationen

ID	TC_Funktion_IFO_17_530
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1404.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1404.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1404.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_530
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1404.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1405 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_531)

3.1405.1 Informationen

ID	TC_Funktion_IFO_17_531
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1405.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1405.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1405.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_531						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1405.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1406 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_532)

3.1406.1 Informationen

ID	TC_Funktion_IFO_17_532
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1406.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1406.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1406.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_532						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1406.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1407 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_533)

3.1407.1 Informationen

ID	TC_Funktion_IFO_17_533
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln

	auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1407.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1407.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1407.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_533						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1407.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1408 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_534)

3.1408.1 Informationen

ID	TC_Funktion_IFO_17_534
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1408.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1408.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1408.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_534						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu

generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'
Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1408.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1409 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_535)

3.1409.1 Informationen

ID	TC_Funktion_IFO_17_535
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1409.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1409.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1409.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_535
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1409.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1410 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_536)

3.1410.1 Informationen

ID	TC_Funktion_IFO_17_536
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1410.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1410.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1410.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_536						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1410.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1411 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_537)

3.1411.1 Informationen

ID	TC_Funktion_IFO_17_537
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'.

	Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1411.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1411.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1411.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_537						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1411.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1412 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_538)

3.1412.1 Informationen

ID	TC_Funktion_IFO_17_538

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1412.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1412.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1412.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_538						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1412.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1413 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_539)

3.1413.1 Informationen

ID	TC_Funktion_IFO_17_539
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1413.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1413.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1413.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_539						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1413.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.1414 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_540)

3.1414.1 Informationen

ID	TC_Funktion_IFO_17_540
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1414.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1414.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1414.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_540 PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1414.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1415 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_541)

3.1415.1 Informationen

ID	TC_Funktion_IFO_17_541
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1415.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1415.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1415.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_541						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1415.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1416 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_542)

3.1416.1 Informationen

ID	TC_Funktion_IFO_17_542
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1416.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1416.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1416.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_542						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1416.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1417 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_543)

3.1417.1 Informationen

ID	TC_Funktion_IFO_17_543
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1417.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1417.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1417.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_543						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1417.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1418 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_544)

3.1418.1 Informationen

ID	TC_Funktion_IFO_17_544
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'PSO

	VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1418.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1418.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1418.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_544						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1418.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1419 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_545)

3.1419.1 Informationen

ID	TC_Funktion_IFO_17_545

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1419.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1419.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1419.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_545						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1419.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1420 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_546)

3.1420.1 Informationen

ID	TC_Funktion_IFO_17_546
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_SIG, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1420.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1420.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1420.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_546						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1420.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1421 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_547)

3.1421.1 Informationen

ID	TC_Funktion_IFO_17_547
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1421.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1421.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1421.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_547						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1421.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1422 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_548)

3.1422.1 Informationen

ID	TC_Funktion_IFO_17_548
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1422.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1422.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1422.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_548
ACTIVATE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1422.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1423 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_549)

3.1423.1 Informationen

ID	TC_Funktion_IFO_17_549
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1423.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1423.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1423.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_549						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1423.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1424 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_550)

3.1424.1 Informationen

ID	TC_Funktion_IFO_17_550
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1424.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1424.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1424.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_550						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1424.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1425 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_551)

3.1425.1 Informationen

ID	TC_Funktion_IFO_17_551
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1425.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1425.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1425.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_551						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1425.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1426 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_552)

3.1426.1 Informationen

ID	TC_Funktion_IFO_17_552
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando

	'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1426.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1426.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1426.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_552						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1426.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1427 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_553)

3.1427.1 Informationen

ID	TC_Funktion_IFO_17_553

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1427.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1427.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1427.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_553						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1427.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1428 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_554)

3.1428.1 Informationen

ID	TC_Funktion_IFO_17_554
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1428.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1428.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1428.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_554 DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1428.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1429 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_555)

3.1429.1 Informationen

ID	TC_Funktion_IFO_17_555
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1429.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1429.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1429.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_555						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1429.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1430 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_556)

3.1430.1 Informationen

ID	TC_Funktion_IFO_17_556
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1430.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1430.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1430.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_556
DELETE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1430.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1431 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_557)

3.1431.1 Informationen

ID	TC_Funktion_IFO_17_557
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1431.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1431.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1431.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_557						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1431.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1432 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_558)

3.1432.1 Informationen

ID	TC_Funktion_IFO_17_558
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1432.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1432.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1432.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_558						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1432.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1433 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_559)

3.1433.1 Informationen

ID	TC_Funktion_IFO_17_559
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1433.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1433.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1433.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_559 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1433.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1434 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_560)

3.1434.1 Informationen

ID	TC_Funktion_IFO_17_560
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.1434.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1434.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1434.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_560						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1434.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1435 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_561)

3.1435.1 Informationen

ID	TC_Funktion_IFO_17_561
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1435.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1435.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1435.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_561 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve)

86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1435.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1436 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_562)

3.1436.1 Informationen

ID	TC_Funktion_IFO_17_562
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1436.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1436.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1436.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_562						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le

00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1436.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1437 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_563)

3.1437.1 Informationen

ID	TC_Funktion_IFO_17_563
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1437.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1437.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1437.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_563						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1437.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1438 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_564)

3.1438.1 Informationen

ID	TC_Funktion_IFO_17_564
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in

	der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1438.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1438.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1438.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_564						
GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1438.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1439 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_565)

3.1439.1 Informationen

ID	TC_Funktion_IFO_17_565
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1439.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1439.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1439.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_565 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1439.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1440 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_566)

3.1440.1 Informationen

ID	TC_Funktion_IFO_17_566
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1440.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1440.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1440.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_566 GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1440.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1441 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_567)

3.1441.1 Informationen

ID	TC_Funktion_IFO_17_567
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1441.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1441.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1441.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_567
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1441.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1442 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_568)

3.1442.1 Informationen

ID	TC_Funktion_IFO_17_568
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1442.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1442.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1442.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_568						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1442.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1443 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_569)

3.1443.1 Informationen

ID	TC_Funktion_IFO_17_569
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1443.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1443.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1443.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_569						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1443.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1444 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_570)

3.1444.1 Informationen

ID	TC_Funktion_IFO_17_570
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln

	auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1444.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1444.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1444.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_570						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1444.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1445 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_571)

3.1445.1 Informationen

ID	TC_Funktion_IFO_17_571
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1445.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1445.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1445.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_571						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu

generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'
Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1445.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1446 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_572)

3.1446.1 Informationen

ID	TC_Funktion_IFO_17_572
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1446.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1446.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1446.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_572
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1446.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1447 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_573)

3.1447.1 Informationen

ID	TC_Funktion_IFO_17_573
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1447.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1447.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1447.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_573						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1447.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1448 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_574)

3.1448.1 Informationen

ID	TC_Funktion_IFO_17_574
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'.

	Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1448.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1448.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1448.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_574						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1448.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1449 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_575)

3.1449.1 Informationen

ID	TC_Funktion_IFO_17_575

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1449.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1449.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1449.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_575						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1449.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1450 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_576)

3.1450.1 Informationen

ID	TC_Funktion_IFO_17_576
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1450.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1450.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1450.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_576						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1450.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.1451 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_577)

3.1451.1 Informationen

ID	TC_Funktion_IFO_17_577
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1451.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1451.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1451.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_577						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1451.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1452 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_578)

3.1452.1 Informationen

ID	TC_Funktion_IFO_17_578
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1452.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1452.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1452.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_578						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1452.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1453 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_579)

3.1453.1 Informationen

ID	TC_Funktion_IFO_17_579
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1453.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1453.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1453.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_579						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1453.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1454 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_580)

3.1454.1 Informationen

ID	TC_Funktion_IFO_17_580
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1454.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1454.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1454.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_580						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1454.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1455 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_581)

3.1455.1 Informationen

ID	TC_Funktion_IFO_17_581
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'PSO

	VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1455.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1455.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1455.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_581						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1455.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1456 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_582)

3.1456.1 Informationen

ID	TC_Funktion_IFO_17_582

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1456.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1456.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1456.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_582						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1456.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1457 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_583)

3.1457.1 Informationen

ID	TC_Funktion_IFO_17_583
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.WAN_ENC, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1457.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1457.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1457.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_583 PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1457.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1458 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_584)

3.1458.1 Informationen

ID	TC_Funktion_IFO_17_584
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1458.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1458.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1458.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_584						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1458.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1459 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_585)

3.1459.1 Informationen

ID	TC_Funktion_IFO_17_585
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1459.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1459.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1459.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_585

ACTIVATE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1459.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1460 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_586)

3.1460.1 Informationen

ID	TC_Funktion_IFO_17_586
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1460.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1460.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1460.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_586						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1460.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1461 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_587)

3.1461.1 Informationen

ID	TC_Funktion_IFO_17_587
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1461.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1461.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1461.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_587						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1461.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1462 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_588)

3.1462.1 Informationen

ID	TC_Funktion_IFO_17_588
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1462.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1462.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1462.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_588						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1462.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1463 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_589)

3.1463.1 Informationen

ID	TC_Funktion_IFO_17_589
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'DEACTIVATE

	KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1463.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1463.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1463.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_589						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1463.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1464 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_590)

3.1464.1 Informationen

ID	TC_Funktion_IFO_17_590

Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1464.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1464.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1464.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_590						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1464.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1465 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_591)

3.1465.1 Informationen

ID	TC_Funktion_IFO_17_591
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1465.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1465.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1465.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_591 DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1465.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1466 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_592)

3.1466.1 Informationen

ID	TC_Funktion_IFO_17_592
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1466.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1466.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1466.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_592 DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1466.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1467 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_593)

3.1467.1 Informationen

ID	TC_Funktion_IFO_17_593
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1467.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1467.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1467.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_593
DELETE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1467.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1468 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_594)

3.1468.1 Informationen

ID	TC_Funktion_IFO_17_594
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1468.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1468.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1468.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_594						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1468.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1469 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_595)

3.1469.1 Informationen

ID	TC_Funktion_IFO_17_595
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1469.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1469.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1469.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_595							
EXTERNAL AUTHENTICATE							
CLA	INS	P1	P2	Lc	Data	Le	
00	82	00	00	LL	XX...XX	XX	

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1469.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1470 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_596)

3.1470.1 Informationen

ID	TC_Funktion_IFO_17_596
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1470.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1470.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1470.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_596						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1470.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1471 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_597)

3.1471.1 Informationen

ID	TC_Funktion_IFO_17_597
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.1471.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1471.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1471.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_597						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1471.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1472 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_598)

3.1472.1 Informationen

ID	TC_Funktion_IFO_17_598
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1472.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1472.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1472.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_598 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit

SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1472.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1473 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_599)

3.1473.1 Informationen

ID	TC_Funktion_IFO_17_599
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1473.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1473.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1473.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_599						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le

00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1473.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1474 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_600)

3.1474.1 Informationen

ID	TC_Funktion_IFO_17_600
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1474.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1474.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1474.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_600						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1474.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1475 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_601)

3.1475.1 Informationen

ID	TC_Funktion_IFO_17_601
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in

	der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1475.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1475.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1475.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_601 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1475.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1476 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_602)

3.1476.1 Informationen

ID	TC_Funktion_IFO_17_602
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1476.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1476.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1476.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_602 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1476.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1477 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_603)

3.1477.1 Informationen

ID	TC_Funktion_IFO_17_603
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1477.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1477.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1477.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_603 GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1477.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1478 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_604)

3.1478.1 Informationen

ID	TC_Funktion_IFO_17_604
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1478.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1478.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1478.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_604
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1478.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1479 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_605)

3.1479.1 Informationen

ID	TC_Funktion_IFO_17_605
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1479.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1479.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1479.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_605						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1479.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1480 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_606)

3.1480.1 Informationen

ID	TC_Funktion_IFO_17_606
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1480.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1480.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1480.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_606						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1480.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1481 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_607)

3.1481.1 Informationen

ID	TC_Funktion_IFO_17_607
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln

	auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1481.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1481.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1481.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_607						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1481.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1482 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_608)

3.1482.1 Informationen

ID	TC_Funktion_IFO_17_608
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1482.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1482.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1482.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_608						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu

generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'
Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1482.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1483 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_609)

3.1483.1 Informationen

ID	TC_Funktion_IFO_17_609
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1483.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1483.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1483.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_609
INTERNAL AUTHENTICATE

CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1483.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1484 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_610)

3.1484.1 Informationen

ID	TC_Funktion_IFO_17_610
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1484.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1484.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1484.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_610						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1484.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1485 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_611)

3.1485.1 Informationen

ID	TC_Funktion_IFO_17_611
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1485.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1485.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1485.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_611						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1485.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1486 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_612)

3.1486.1 Informationen

ID	TC_Funktion_IFO_17_612
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1486.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1486.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1486.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_612						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1486.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1487 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_613)

3.1487.1 Informationen

ID	TC_Funktion_IFO_17_613
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.1487.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1487.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1487.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_613 PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1487.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1488 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_614)

3.1488.1 Informationen

ID	TC_Funktion_IFO_17_614
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1488.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1488.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1488.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_614						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1488.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1489 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_615)

3.1489.1 Informationen

ID	TC_Funktion_IFO_17_615
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1489.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1489.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1489.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_615						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1489.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1490 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_616)

3.1490.1 Informationen

ID	TC_Funktion_IFO_17_616
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1490.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1490.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1490.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_616
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1490.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1491 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_617)

3.1491.1 Informationen

ID	TC_Funktion_IFO_17_617
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.CA_x, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand - je nachdem, ob das PIN-Objekt für die GW-System-PIN aktiviert wurde und die Nutzung von PACE erzwungen ist.
Klassifizierung	Gutfall-Test

3.1491.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1491.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1491.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_617						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1491.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1492 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_618)

3.1492.1 Informationen

ID	TC_Funktion_IFO_17_618
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1492.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1492.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1492.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_618						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1492.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1493 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_619)

3.1493.1 Informationen

ID	TC_Funktion_IFO_17_619
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'.

	Die Durchführung erfolgt für Key.EPH_1, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1493.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1493.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1493.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_619						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1493.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1494 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_620)

3.1494.1 Informationen

ID	TC_Funktion_IFO_17_620
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1494.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1494.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1494.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_620 CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1494.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1495 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_621)

3.1495.1 Informationen

ID	TC_Funktion_IFO_17_621
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1495.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1495.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1495.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_621						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1495.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1496 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_622)

3.1496.1 Informationen

ID	TC_Funktion_IFO_17_622
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1496.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1496.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1496.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_622						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le

00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1496.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1497 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_623)

3.1497.1 Informationen

ID	TC_Funktion_IFO_17_623
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1497.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1497.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1497.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_623						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1497.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1498 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_624)

3.1498.1 Informationen

ID	TC_Funktion_IFO_17_624
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1498.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1498.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1498.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_624						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1498.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1499 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_625)

3.1499.1 Informationen

ID	TC_Funktion_IFO_17_625
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1499.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1499.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1499.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_625						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1499.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1500 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_626)

3.1500.1 Informationen

ID	TC_Funktion_IFO_17_626
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'.

	Die Durchführung erfolgt für Key.EPH_1, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1500.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1500.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1500.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_626 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1500.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1501 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_627)

3.1501.1 Informationen

ID	TC_Funktion_IFO_17_627
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen

	Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1501.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1501.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1501.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_627 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1501.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1502 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_628)

3.1502.1 Informationen

ID	TC_Funktion_IFO_17_628
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1502.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1502.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1502.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_628 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit

SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1502.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1503 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_629)

3.1503.1 Informationen

ID	TC_Funktion_IFO_17_629
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1503.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1503.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1503.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_629						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le

00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1503.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1504 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_630)

3.1504.1 Informationen

ID	TC_Funktion_IFO_17_630
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1504.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1504.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1504.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_630						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1504.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1505 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_631)

3.1505.1 Informationen

ID	TC_Funktion_IFO_17_631
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.

Klassifizierung	Fehlerfall-Test

3.1505.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1505.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1505.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_631						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1505.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1506 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_632)

3.1506.1 Informationen

ID	TC_Funktion_IFO_17_632
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1506.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1506.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1506.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_632 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1506.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1507 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_633)

3.1507.1 Informationen

ID	TC_Funktion_IFO_17_633
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1507.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1507.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1507.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_633 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1507.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1508 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_634)

3.1508.1 Informationen

ID	TC_Funktion_IFO_17_634
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1508.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1508.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1508.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_634						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1508.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1509 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_635)

3.1509.1 Informationen

ID	TC_Funktion_IFO_17_635
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1509.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1509.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1509.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_635						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1509.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1510 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_636)

3.1510.1 Informationen

ID	TC_Funktion_IFO_17_636
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1510.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1510.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1510.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_636						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1510.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1511 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_637)

3.1511.1 Informationen

ID	TC_Funktion_IFO_17_637
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln

	auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1511.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1511.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1511.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_637						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1511.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1512 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_638)

3.1512.1 Informationen

ID	TC_Funktion_IFO_17_638
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1512.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1512.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1512.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_638						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu

generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'
Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1512.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1513 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_639)

3.1513.1 Informationen

ID	TC_Funktion_IFO_17_639
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1513.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1513.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1513.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_639
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1513.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1514 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_640)

3.1514.1 Informationen

ID	TC_Funktion_IFO_17_640
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1514.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1514.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1514.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_640						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1514.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1515 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_641)

3.1515.1 Informationen

ID	TC_Funktion_IFO_17_641
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1515.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1515.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1515.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_641 INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1515.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1516 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_642)

3.1516.1 Informationen

ID	TC_Funktion_IFO_17_642
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.1516.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1516.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1516.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_642 PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1516.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1517 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_643)

3.1517.1 Informationen

ID	TC_Funktion_IFO_17_643
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln

	auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1517.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1517.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1517.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_643						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1517.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1518 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_644)

3.1518.1 Informationen

ID	TC_Funktion_IFO_17_644
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1518.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1518.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1518.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_644						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1518.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1519 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_645)

3.1519.1 Informationen

ID	TC_Funktion_IFO_17_645
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1519.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1519.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1519.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_645						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1519.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1520 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_646)

3.1520.1 Informationen

ID	TC_Funktion_IFO_17_646
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1520.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1520.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1520.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_646						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1520.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1521 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_647)

3.1521.1 Informationen

ID	TC_Funktion_IFO_17_647
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1521.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1521.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1521.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_647						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1521.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1522 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_648)

3.1522.1 Informationen

ID	TC_Funktion_IFO_17_648
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1522.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1522.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1522.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_648						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1522.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1523 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_649)

3.1523.1 Informationen

ID	TC_Funktion_IFO_17_649
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in

	der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_1, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1523.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1523.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1523.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_649						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1523.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1524 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_650)

3.1524.1 Informationen

ID	TC_Funktion_IFO_17_650
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1524.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1524.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1524.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_650 ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1524.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1525 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_651)

3.1525.1 Informationen

ID	TC_Funktion_IFO_17_651
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1525.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1525.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1525.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_651						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1525.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1526 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_652)

3.1526.1 Informationen

ID	TC_Funktion_IFO_17_652
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1526.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1526.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1526.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_652
CREATE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1526.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1527 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_653)

3.1527.1 Informationen

ID	TC_Funktion_IFO_17_653
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1527.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1527.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1527.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_653						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1527.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1528 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_654)

3.1528.1 Informationen

ID	TC_Funktion_IFO_17_654
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1528.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1528.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1528.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_654						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1528.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1529 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_655)

3.1529.1 Informationen

ID	TC_Funktion_IFO_17_655
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1529.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1529.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1529.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_655						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1529.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1530 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_656)

3.1530.1 Informationen

ID	TC_Funktion_IFO_17_656
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'.

	Die Durchführung erfolgt für Key.EPH_2, das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1530.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1530.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1530.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_656						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1530.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1531 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_657)

3.1531.1 Informationen

ID	TC_Funktion_IFO_17_657
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1531.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1531.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1531.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_657 DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1531.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1532 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_658)

3.1532.1 Informationen

ID	TC_Funktion_IFO_17_658
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1532.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1532.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1532.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_658						
EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1532.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1533 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_659)

3.1533.1 Informationen

ID	TC_Funktion_IFO_17_659
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1533.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1533.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1533.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_659 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1533.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1534 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_660)

3.1534.1 Informationen

ID	TC_Funktion_IFO_17_660
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1534.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1534.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1534.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_660 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le

00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1534.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1535 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_661)

3.1535.1 Informationen

ID	TC_Funktion_IFO_17_661
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1535.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1535.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1535.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_661						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1535.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1536 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_662)

3.1536.1 Informationen

ID	TC_Funktion_IFO_17_662
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1536.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1536.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1536.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_662						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1536.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1537 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_663)

3.1537.1 Informationen

ID	TC_Funktion_IFO_17_663
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1537.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1537.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1537.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_663 GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator

sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1537.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1538 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_664)

3.1538.1 Informationen

ID	TC_Funktion_IFO_17_664
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1538.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1538.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1538.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_664							
GENERAL AUTHENTICATE (PACE)							
CLA	INS	P1	P2	Lc	Data	Le	

XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1538.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1539 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_665)

3.1539.1 Informationen

ID	TC_Funktion_IFO_17_665
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'GENERAL AUTHENTICATE (PACE)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1539.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1539.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1539.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_665						
GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1539.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1540 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_666)

3.1540.1 Informationen

ID	TC_Funktion_IFO_17_666
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1540.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1540.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1540.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_666						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1540.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1541 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_667)

3.1541.1 Informationen

ID	TC_Funktion_IFO_17_667
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1541.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1541.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1541.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_667 GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1541.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1542 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_668)

3.1542.1 Informationen

ID	TC_Funktion_IFO_17_668
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'GENERATE

	ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1542.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1542.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1542.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_668						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1542.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1543 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_669)

3.1543.1 Informationen

ID	TC_Funktion_IFO_17_669
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1543.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1543.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1543.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_669						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1543.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1544 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_670)

3.1544.1 Informationen

ID	TC_Funktion_IFO_17_670
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1544.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1544.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1544.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_670						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1544.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1545 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_671)

3.1545.1 Informationen

ID	TC_Funktion_IFO_17_671
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1545.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1545.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1545.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_671						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1545.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1546 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_672)

3.1546.1 Informationen

ID	TC_Funktion_IFO_17_672
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1546.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1546.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1546.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_672 INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1546.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1547 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_673)

3.1547.1 Informationen

ID	TC_Funktion_IFO_17_673
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.

Klassifizierung	Fehlerfall-Test

3.1547.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1547.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1547.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_673						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1547.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1548 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_674)

3.1548.1 Informationen

ID	TC_Funktion_IFO_17_674
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln

	auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1548.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1548.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1548.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_674						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1548.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1549 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_675)

3.1549.1 Informationen

ID	TC_Funktion_IFO_17_675
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1549.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1549.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1549.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_675						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1549.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.1550 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_676)

3.1550.1 Informationen

ID	TC_Funktion_IFO_17_676
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1550.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1550.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1550.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_676 PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public

Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1550.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1551 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_677)

3.1551.1 Informationen

ID	TC_Funktion_IFO_17_677
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1551.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1551.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1551.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_677						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le

00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1551.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1552 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_678)

3.1552.1 Informationen

ID	TC_Funktion_IFO_17_678
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1552.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1552.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1552.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_678						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1552.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1553 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_679)

3.1553.1 Informationen

ID	TC_Funktion_IFO_17_679
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1553.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1553.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1553.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_679						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1553.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1554 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_680)

3.1554.1 Informationen

ID	TC_Funktion_IFO_17_680
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1554.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1554.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1554.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_680						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1554.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1555 Testfall: Initiales Datei- und Objektsystem (TC_Funktion_IFO_17_681)

3.1555.1 Informationen

ID	TC_Funktion_IFO_17_681
Beschreibung	Es wird getestet, ob Zugriffsrechte auf das DF.SMGW und die initialen Dateien und Objekte korrekt gesetzt sind. Der Testfall prüft Zugriffsregeln auf das DF.SMGW und die initialen Dateien und Objekte im DF.SMGW in

	der Phase 'Personalisierung des SMGW und Normalbetrieb des SMGW'. Die Durchführung erfolgt für Key.EPH_2, das Kommando 'PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1555.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.1, 3.3.3.3

3.1555.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1555.4 APDU-Kommandos

ID: CM-Funktion_IFO_17_681						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1555.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1556 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_1)

3.1556.1 Informationen

ID	TC_Funktion_EFO_1_1
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1556.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1556.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1556.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_1						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1556.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.1557 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_2)

3.1557.1 Informationen

ID	TC_Funktion_EFO_1_2
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1557.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1557.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1557.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_2						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1557.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1558 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_3)

3.1558.1 Informationen

ID	TC_Funktion_EFO_1_3
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CREATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1558.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1558.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1558.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_3 CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1558.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1559 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_4)

3.1559.1 Informationen

ID	TC_Funktion_EFO_1_4
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DELETE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1559.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1559.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1559.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_4						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le

00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1559.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1560 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_5)

3.1560.1 Informationen

ID	TC_Funktion_EFO_1_5
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1560.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1560.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1560.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_5						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1560.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1561 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_6)

3.1561.1 Informationen

ID	TC_Funktion_EFO_1_6
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DELETE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1561.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1561.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1561.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_6						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1561.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1562 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_7)

3.1562.1 Informationen

ID	TC_Funktion_EFO_1_7
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1562.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1562.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1562.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_7						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1562.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1563 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_8)

3.1563.1 Informationen

ID	TC_Funktion_EFO_1_8
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt

	für das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1563.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1563.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1563.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_8						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1563.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1564 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_9)

3.1564.1 Informationen

ID	TC_Funktion_EFO_1_9

Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1564.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1564.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1564.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_9						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1564.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1565 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_10)

3.1565.1 Informationen

ID	TC_Funktion_EFO_1_10
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1565.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1565.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1565.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_10						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1565.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1566 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_11)

3.1566.1 Informationen

ID	TC_Funktion_EFO_1_11
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1566.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1566.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1566.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_11 DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1566.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1567 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_12)

3.1567.1 Informationen

ID	TC_Funktion_EFO_1_12
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1567.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1567.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1567.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_12

DEACTIVATE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1567.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1568 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_13)

3.1568.1 Informationen

ID	TC_Funktion_EFO_1_13
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselgenerierung mit Export des Public Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1568.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1568.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1568.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_13						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1568.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1569 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_14)

3.1569.1 Informationen

ID	TC_Funktion_EFO_1_14
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselgenerierung mit Export des Public Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1569.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1569.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1569.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_14						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1569.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1570 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_15)

3.1570.1 Informationen

ID	TC_Funktion_EFO_1_15
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und

	Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselgenerierung mit Export des Public Key)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1570.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1570.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1570.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_15						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1570.5 Erwartete Ergebnisse

ID	Beschreibung

RS-9000	Das Testsystem antwortet mit '90 00'.

3.1571 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_16)

3.1571.1 Informationen

ID	TC_Funktion_EFO_1_16
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselgenerierung ohne Export des Public Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1571.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1571.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1571.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_16						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT):

'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1571.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1572 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_17)

3.1572.1 Informationen

ID	TC_Funktion_EFO_1_17
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselgenerierung ohne Export des Public Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1572.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1572.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1572.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_17
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1572.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1573 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_18)

3.1573.1 Informationen

ID	TC_Funktion_EFO_1_18
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselgenerierung ohne Export des Public Key)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1573.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1573.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1573.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_18						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1573.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1574 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_19)

3.1574.1 Informationen

ID	TC_Funktion_EFO_1_19
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERATE ASYMMETRIC KEY PAIR (nur Schlüsselexport, ohne Schlüsselgenerierung)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1574.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1574.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1574.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_19						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1574.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1575 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_20)

3.1575.1 Informationen

ID	TC_Funktion_EFO_1_20
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den

	Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERATE ASYMMETRIC KEY PAIR (nur Schlüsselexport, ohne Schlüsselgenerierung)' und den Sicherheitszustand PACE.
Klassifizierung	Gutfall-Test

3.1575.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1575.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1575.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_20						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1575.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1576 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_21)

3.1576.1 Informationen

ID	TC_Funktion_EFO_1_21
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1576.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1576.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1576.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_21						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1576.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.1577 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_22)

3.1577.1 Informationen

ID	TC_Funktion_EFO_1_22
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Gutfall-Test

3.1577.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1577.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1577.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_22						
PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1577.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1578 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_23)

3.1578.1 Informationen

ID	TC_Funktion_EFO_1_23
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'PSO VERIFY DIGITAL SIGNATURE (Variante ohne Übergabe des Public Key im Kommando)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1578.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1578.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1578.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_23						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1578.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1579 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_24)

3.1579.1 Informationen

ID	TC_Funktion_EFO_1_24
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'PSO VERIFY DIGITAL SIGNATURE (Variante ohne Übergabe des Public Key im Kommando)' und den Sicherheitszustand PACE.
Klassifizierung	Gutfall-Test

3.1579.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1579.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1579.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_24 PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)

CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1579.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1580 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_25)

3.1580.1 Informationen

ID	TC_Funktion_EFO_1_25
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'PSO VERIFY DIGITAL SIGNATURE (Variante mit Übergabe des Public Key im Kommando)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand, abhängig vom CLA-Byte des Kommandos.
Klassifizierung	

3.1580.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1580.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1580.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_25						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1580.5 Erwartete Ergebnisse

ID	Beschreibung
RS-E718	69 82 oder 90 00, abhängig vom CLA-Byte des Kommandos

3.1581 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_26)

3.1581.1 Informationen

ID	TC_Funktion_EFO_1_26
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1581.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1581.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1581.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_26						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1581.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1582 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_27)

3.1582.1 Informationen

ID	TC_Funktion_EFO_1_27
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.

Klassifizierung	Fehlerfall-Test

3.1582.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1582.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1582.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_27						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1582.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1583 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_28)

3.1583.1 Informationen

ID	TC_Funktion_EFO_1_28

Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1583.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1583.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1583.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_28						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1583.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1584 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_29)

3.1584.1 Informationen

ID	TC_Funktion_EFO_1_29
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1584.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1584.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1584.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_29						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve)

86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1584.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1585 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_30)

3.1585.1 Informationen

ID	TC_Funktion_EFO_1_30
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1585.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1585.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1585.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_30						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le

00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1585.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1586 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_31)

3.1586.1 Informationen

ID	TC_Funktion_EFO_1_31
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1586.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1586.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1586.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_31						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1586.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1587 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_32)

3.1587.1 Informationen

ID	TC_Funktion_EFO_1_32
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW"

	den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1587.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1587.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1587.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_32 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1587.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1588 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_33)

3.1588.1 Informationen

ID	TC_Funktion_EFO_1_33
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1588.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1588.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1588.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_33 GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit

SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1588.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1589 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_34)

3.1589.1 Informationen

ID	TC_Funktion_EFO_1_34
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1589.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1589.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1589.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_34						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le

00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1589.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1590 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_35)

3.1590.1 Informationen

ID	TC_Funktion_EFO_1_35
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1590.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1590.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1590.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_35 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1590.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1591 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_36)

3.1591.1 Informationen

ID	TC_Funktion_EFO_1_36
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1591.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1591.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1591.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_36 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1591.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1592 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_37)

3.1592.1 Informationen

ID	TC_Funktion_EFO_1_37
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW"

	den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1592.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1592.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1592.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_37 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1592.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1593 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_38)

3.1593.1 Informationen

ID	TC_Funktion_EFO_1_38
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1593.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1593.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1593.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_38 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1593.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1594 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_39)

3.1594.1 Informationen

ID	TC_Funktion_EFO_1_39
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Gutfall-Test

3.1594.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1594.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1594.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_39 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1594.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1595 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_40)

3.1595.1 Informationen

ID	TC_Funktion_EFO_1_40
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1595.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1595.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1595.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_40 INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1595.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.1596 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_1_41)

3.1596.1 Informationen

ID	TC_Funktion_EFO_1_41
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Gutfall-Test

3.1596.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1596.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1596.4 APDU-Kommandos

ID: CM-Funktion_EFO_1_41 INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1596.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1597 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_2_42)

3.1597.1 Informationen

ID	TC_Funktion_EFO_2_42
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten PIN-Objekten, ob die PIN-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CHANGE REFERENCE DATA (Variante Wechseln einer PIN mit der LCS (PIN-LifeCycleStatus) initialisation)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1597.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1597.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1597.4 APDU-Kommandos

ID: CM-Funktion_EFO_2_42						
CHANGE REFERENCE DATA (Wechseln einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

3.1597.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1598 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_2_43)

3.1598.1 Informationen

ID	TC_Funktion_EFO_2_43
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten PIN-Objekten, ob die PIN-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CHANGE REFERENCE DATA (Variante Wechseln einer PIN mit der LCS (PIN-LifeCycleStatus) initialisation)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1598.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1598.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1598.4 APDU-Kommandos

ID: CM-Funktion_EFO_2_43
CHANGE REFERENCE DATA (Wechseln einer PIN)

CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

3.1598.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1599 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_2_44)

3.1599.1 Informationen

ID	TC_Funktion_EFO_2_44
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten PIN-Objekten, ob die PIN-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CHANGE REFERENCE DATA (Variante Wechseln einer PIN mit der LCSI (PIN-LifeCycleStatus) initialisation)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1599.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1599.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1599.4 APDU-Kommandos

ID: CM-Funktion_EFO_2_44						
CHANGE REFERENCE DATA (Wechseln einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

3.1599.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1600 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_2_45)

3.1600.1 Informationen

ID	TC_Funktion_EFO_2_45
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten PIN-Objekten, ob die PIN-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CHANGE REFERENCE DATA (Variante Wechseln einer PIN mit der LCS (PIN-LifeCycleStatus) operational state - activated)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1600.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1600.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1600.4 APDU-Kommandos

ID: CM-Funktion_EFO_2_45						
CHANGE REFERENCE DATA (Wechseln einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

3.1600.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1601 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_2_46)

3.1601.1 Informationen

ID	TC_Funktion_EFO_2_46
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten PIN-Objekten, ob die PIN-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CHANGE REFERENCE DATA (Variante Wechseln einer PIN mit der LCSI (PIN-LifeCycleStatus) operational state - activated)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1601.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1601.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1601.4 APDU-Kommandos

ID: CM-Funktion_EFO_2_46 CHANGE REFERENCE DATA (Wechseln einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

3.1601.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1602 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_2_47)

3.1602.1 Informationen

ID	TC_Funktion_EFO_2_47
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten PIN-Objekten, ob die PIN-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CHANGE REFERENCE DATA (Variante Wechseln einer PIN mit der LCSI (PIN-LifeCycleStatus) operational state

	- activated)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1602.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1602.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1602.4 APDU-Kommandos

ID: CM-Funktion_EFO_2_47						
CHANGE REFERENCE DATA (Wechseln einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

3.1602.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1603 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_2_48)

3.1603.1 Informationen

ID	TC_Funktion_EFO_2_48
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im

	MF angelegten PIN-Objekten, ob die PIN-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CHANGE REFERENCE DATA (Variante Wechseln einer PIN)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1603.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1603.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1603.4 APDU-Kommandos

ID: CM-Funktion_EFO_2_48						
CHANGE REFERENCE DATA (Wechseln einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

3.1603.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1604 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_2_49)

3.1604.1 Informationen

ID	TC_Funktion_EFO_2_49
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten PIN-Objekten, ob die PIN-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CHANGE REFERENCE DATA (Variante Wechseln einer PIN)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1604.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1604.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1604.4 APDU-Kommandos

ID: CM-Funktion_EFO_2_49 CHANGE REFERENCE DATA (Wechseln einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

3.1604.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.1605 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_2_50)

3.1605.1 Informationen

ID	TC_Funktion_EFO_2_50
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten PIN-Objekten, ob die PIN-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CHANGE REFERENCE DATA (Variante Wechseln einer PIN)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1605.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1605.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1605.4 APDU-Kommandos

ID: CM-Funktion_EFO_2_50						
CHANGE REFERENCE DATA (Wechseln einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

3.1605.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1606 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_2_51)

3.1606.1 Informationen

ID	TC_Funktion_EFO_2_51
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten PIN-Objekten, ob die PIN-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CHANGE REFERENCE DATA (Variante Setzen einer PIN)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1606.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1606.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1606.4 APDU-Kommandos

ID: CM-Funktion_EFO_2_51 CHANGE REFERENCE DATA (Setzen einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	01	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die neue PIN.

3.1606.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1607 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_2_52)

3.1607.1 Informationen

ID	TC_Funktion_EFO_2_52
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten PIN-Objekten, ob die PIN-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CHANGE REFERENCE DATA (Variante Setzen einer PIN)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1607.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1607.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1607.4 APDU-Kommandos

ID: CM-Funktion_EFO_2_52						
CHANGE REFERENCE DATA (Setzen einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	01	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die neue PIN.

3.1607.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1608 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_2_53)

3.1608.1 Informationen

ID	TC_Funktion_EFO_2_53
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten PIN-Objekten, ob die PIN-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CHANGE REFERENCE DATA (Variante Setzen einer PIN)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1608.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1608.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1608.4 APDU-Kommandos

ID: CM-Funktion_EFO_2_53

CHANGE REFERENCE DATA (Setzen einer PIN)

CLA	INS	P1	P2	Lc	Data	Le
00	24	01	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die neue PIN.

3.1608.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1609 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_54)

3.1609.1 Informationen

ID	TC_Funktion_EFO_3_54
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ BINARY (für nicht initiale EF mit LCSi initialisation)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1609.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1609.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1609.4 APDU-Kommandos

ID: CM-Funktion_EFO_3_54						
READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1609.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1610 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_55)

3.1610.1 Informationen

ID	TC_Funktion_EFO_3_55
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ BINARY (für nicht initiale EF mit LCSi operational state - activated)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1610.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1610.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1610.4 APDU-Kommandos

ID: CM-Funktion_EFO_3_55						
READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1610.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1611 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_56)

3.1611.1 Informationen

ID	TC_Funktion_EFO_3_56
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ BINARY (für nicht initiale EF mit LCSi operational state - deactivated)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1611.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1611.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1611.4 APDU-Kommandos

ID: CM-Funktion_EFO_3_56						
READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1611.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1612 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_57)

3.1612.1 Informationen

ID	TC_Funktion_EFO_3_57
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ BINARY (für nicht initiale EF mit LCSI operational state - deactivated)' und den

	Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1612.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1612.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1612.4 APDU-Kommandos

ID: CM-Funktion_EFO_3_57 READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1612.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1613 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_58)

3.1613.1 Informationen

ID	TC_Funktion_EFO_3_58
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im

	MF angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ BINARY (für nicht initiale EF mit LCSi operational state - deactivated)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1613.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1613.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1613.4 APDU-Kommandos

ID: CM-Funktion_EFO_3_58 READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1613.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1614 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_59)

3.1614.1 Informationen

ID	TC_Funktion_EFO_3_59
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ BINARY (für nicht initiale EF mit LCSi terminated)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1614.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1614.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1614.4 APDU-Kommandos

ID: CM-Funktion_EFO_3_59 READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1614.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.1615 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_60)

3.1615.1 Informationen

ID	TC_Funktion_EFO_3_60
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ BINARY (für nicht initiale EF mit LCSi terminated)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1615.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1615.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1615.4 APDU-Kommandos

ID: CM-Funktion_EFO_3_60 READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1615.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1616 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_61)

3.1616.1 Informationen

ID	TC_Funktion_EFO_3_61
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ BINARY (für nicht initiale EF mit LCSi terminated)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1616.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1616.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1616.4 APDU-Kommandos

ID: CM-Funktion_EFO_3_61						
READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1616.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1617 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_62)

3.1617.1 Informationen

ID	TC_Funktion_EFO_3_62
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE BINARY (für nicht initiale EF mit LCSi initialisation)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1617.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1617.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1617.4 APDU-Kommandos

ID: CM-Funktion_EFO_3_62
UPDATE RECORD (ohne SFI)

CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1617.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1618 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_63)

3.1618.1 Informationen

ID	TC_Funktion_EFO_3_63
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE BINARY (für nicht initiale EF mit LCSI operational state - activated)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1618.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1618.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1618.4 APDU-Kommandos

ID: CM-Funktion_EFO_3_63						
UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1618.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1619 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_64)

3.1619.1 Informationen

ID	TC_Funktion_EFO_3_64
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE BINARY (für nicht initiale EF mit LCSI operational state - deactivated)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1619.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1619.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1619.4 APDU-Kommandos

ID: CM-Funktion_EFO_3_64						
UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1619.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1620 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_65)

3.1620.1 Informationen

ID	TC_Funktion_EFO_3_65
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE BINARY (für nicht initiale EF mit LCSI operational state - deactivated)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1620.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1620.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1620.4 APDU-Kommandos

ID: CM-Funktion_EFO_3_65 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1620.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1621 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_66)

3.1621.1 Informationen

ID	TC_Funktion_EFO_3_66
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen

	genügen. Die Durchführung erfolgt für das Kommando 'UPDATE BINARY (für nicht initiale EF mit LCSI operational state - deactivated)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1621.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1621.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1621.4 APDU-Kommandos

ID: CM-Funktion_EFO_3_66 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1621.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1622 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_67)

3.1622.1 Informationen

ID	TC_Funktion_EFO_3_67
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE BINARY (für nicht initiale EF mit LCSi terminated)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1622.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1622.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1622.4 APDU-Kommandos

ID: CM-Funktion_EFO_3_67 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1622.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1623 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_68)

3.1623.1 Informationen

ID	TC_Funktion_EFO_3_68
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE BINARY (für nicht initiale EF mit LCSi terminated)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1623.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1623.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1623.4 APDU-Kommandos

ID: CM-Funktion_EFO_3_68 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1623.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1624 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_3_69)

3.1624.1 Informationen

ID	TC_Funktion_EFO_3_69
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE BINARY (für nicht initiale EF mit LCSi terminated)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1624.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1624.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1624.4 APDU-Kommandos

ID: CM-Funktion_EFO_3_69 UPDATE BINARY (ohne SFI)

CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1624.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1625 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_70)

3.1625.1 Informationen

ID	TC_Funktion_EFO_4_70
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ RECORD (für nicht initiale record-orientierte EF mit LCSi initialisation)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1625.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1625.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1625.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_70						
READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1625.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1626 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_71)

3.1626.1 Informationen

ID	TC_Funktion_EFO_4_71
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ RECORD (für nicht initiale record-orientierte EF mit LCSi initialisation)' und den Sicherheitszustand PACE.
Klassifizierung	Gutfall-Test

3.1626.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1626.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1626.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_71 READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1626.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1627 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_72)

3.1627.1 Informationen

ID	TC_Funktion_EFO_4_72
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ RECORD (für nicht initiale record-orientierte EF mit LCSi operational state - activated)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1627.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1627.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1627.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_72 READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1627.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1628 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_73)

3.1628.1 Informationen

ID	TC_Funktion_EFO_4_73
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ RECORD (für nicht initiale record-orientierte EF mit LCSi operational state - activated)' und den Sicherheitszustand PACE.
Klassifizierung	Gutfall-Test

3.1628.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1628.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1628.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_73						
READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1628.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1629 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_74)

3.1629.1 Informationen

ID	TC_Funktion_EFO_4_74
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ RECORD (für nicht initiale record-orientierte EF mit LCS operation state - deactivated)' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.1629.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1629.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1629.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_74						
READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1629.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1630 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_75)

3.1630.1 Informationen

ID	TC_Funktion_EFO_4_75
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen

	genügen. Die Durchführung erfolgt für das Kommando 'READ RECORD (für nicht initiale record-orientierte EF mit LCSI operation state - deactivated)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1630.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1630.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1630.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_75 READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1630.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1631 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_76)

3.1631.1 Informationen

ID	TC_Funktion_EFO_4_76
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und

	Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ RECORD (für nicht initiale record-orientierte EF mit LCS operation state - deactivated)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1631.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1631.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1631.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_76						
READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1631.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1632 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_77)

3.1632.1 Informationen

ID	TC_Funktion_EFO_4_77
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ RECORD (für nicht initiale record-orientierte EF mit LCS terminated)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1632.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1632.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1632.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_77						
READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1632.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.1633 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_78)

3.1633.1 Informationen

ID	TC_Funktion_EFO_4_78
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ RECORD (für nicht initiale record-orientierte EF mit LCSi terminated)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1633.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1633.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1633.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_78						
READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1633.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1634 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_79)

3.1634.1 Informationen

ID	TC_Funktion_EFO_4_79
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ RECORD (für nicht initiale record-orientierte EF mit LCSi terminated)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1634.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1634.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1634.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_79						
READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1634.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1635 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_80)

3.1635.1 Informationen

ID	TC_Funktion_EFO_4_80
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE RECORD (für nicht initiale record-orientierte EF mit LCSi initialisation)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1635.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1635.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1635.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_80						
UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le

00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1635.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1636 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_81)

3.1636.1 Informationen

ID	TC_Funktion_EFO_4_81
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE RECORD (für nicht initiale record-orientierte EF mit LCSi initialisation)' und den Sicherheitszustand PACE.
Klassifizierung	Gutfall-Test

3.1636.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1636.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1636.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_81						
UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1636.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1637 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_82)

3.1637.1 Informationen

ID	TC_Funktion_EFO_4_82
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE RECORD (für nicht initiale record-orientierte EF mit LCSi operational state - activated)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1637.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1637.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1637.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_82 UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1637.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1638 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_83)

3.1638.1 Informationen

ID	TC_Funktion_EFO_4_83
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE RECORD (für nicht initiale record-orientierte EF mit LCSi operational state - activated)' und den Sicherheitszustand PACE.
Klassifizierung	Gutfall-Test

3.1638.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1638.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1638.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_83 UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1638.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1639 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_84)

3.1639.1 Informationen

ID	TC_Funktion_EFO_4_84
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE RECORD (für nicht initiale record-orientierte EF mit LCSI operational

	state - deactivated)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1639.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1639.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1639.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_84 UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1639.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1640 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_85)

3.1640.1 Informationen

ID	TC_Funktion_EFO_4_85
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im

	MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE RECORD (für nicht initiale record-orientierte EF mit LCSi operational state - deactivated)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1640.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1640.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1640.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_85 UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1640.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1641 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_86)

3.1641.1 Informationen

ID	TC_Funktion_EFO_4_86
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE RECORD (für nicht initiale record-orientierte EF mit LCSi operational state - deactivated)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1641.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1641.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1641.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_86 UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1641.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1642 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_87)

3.1642.1 Informationen

ID	TC_Funktion_EFO_4_87
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE RECORD (für nicht initiale record-orientierte EF mit LCS terminated)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1642.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1642.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1642.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_87 UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1642.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1643 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_88)

3.1643.1 Informationen

ID	TC_Funktion_EFO_4_88
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE RECORD (für nicht initiale record-orientierte EF mit LCSI terminated)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1643.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1643.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1643.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_88 UPDATE RECORD (ohne SFI)

CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1643.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1644 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_89)

3.1644.1 Informationen

ID	TC_Funktion_EFO_4_89
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE RECORD (für nicht initiale record-orientierte EF mit LCSi terminated)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1644.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1644.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1644.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_89						
UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1644.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1645 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_90)

3.1645.1 Informationen

ID	TC_Funktion_EFO_4_90
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'APPEND RECORD (für nicht initiale record-orientierte EF mit LCSi initialisation, sofern implementiert)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1645.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1645.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1645.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_90 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1645.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1646 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_91)

3.1646.1 Informationen

ID	TC_Funktion_EFO_4_91
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'APPEND RECORD (für nicht initiale record-orientierte EF mit LCSi initialisation, sofern implementiert)' und den Sicherheitszustand PACE.
Klassifizierung	Gutfall-Test

3.1646.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1646.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1646.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_91 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1646.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1647 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_92)

3.1647.1 Informationen

ID	TC_Funktion_EFO_4_92
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'APPEND RECORD (für nicht initiale record-orientierte EF mit LCSi operational state - activated, sofern implementiert)' und ohne Sicherheitszustand.

Klassifizierung	Fehlerfall-Test

3.1647.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1647.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1647.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_92 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1647.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1648 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_93)

3.1648.1 Informationen

ID	TC_Funktion_EFO_4_93
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen

	genügen. Die Durchführung erfolgt für das Kommando 'APPEND RECORD (für nicht initiale record-orientierte EF mit LCSi operational state - activated, sofern implementiert)' und den Sicherheitszustand PACE.
Klassifizierung	Gutfall-Test

3.1648.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1648.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1648.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_93 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1648.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1649 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_94)

3.1649.1 Informationen

ID	TC_Funktion_EFO_4_94
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und

	Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'APPEND RECORD (für nicht initiale record-orientierte EF operational state - deactivated, sofern implementiert)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1649.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1649.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1649.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_94						
APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1649.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1650 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_95)

3.1650.1 Informationen

ID	TC_Funktion_EFO_4_95
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'APPEND RECORD (für nicht initiale record-orientierte EF operational state - deactivated, sofern implementiert)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1650.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1650.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1650.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_95 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1650.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.1651 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_96)

3.1651.1 Informationen

ID	TC_Funktion_EFO_4_96
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'APPEND RECORD (für nicht initiale record-orientierte EFoperational state - deactivated, sofern implementiert)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1651.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1651.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1651.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_96 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1651.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1652 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_97)

3.1652.1 Informationen

ID	TC_Funktion_EFO_4_97
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'APPEND RECORD (für nicht initiale record-orientierte EF LCSII terminated, sofern implementiert)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1652.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1652.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1652.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_97 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1652.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1653 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_98)

3.1653.1 Informationen

ID	TC_Funktion_EFO_4_98
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'APPEND RECORD (für nicht initiale record-orientierte EF LCSi terminated, sofern implementiert)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1653.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1653.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1653.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_98 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le

00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1653.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1654 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_4_99)

3.1654.1 Informationen

ID	TC_Funktion_EFO_4_99
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'APPEND RECORD (für nicht initiale record-orientierte EF LCSI terminated, sofern implementiert)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1654.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1654.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1654.4 APDU-Kommandos

ID: CM-Funktion_EFO_4_99

APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1654.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1655 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_100)

3.1655.1 Informationen

ID	TC_Funktion_EFO_5_100
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'SELECT DF' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1655.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1655.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1655.4 APDU-Kommandos

ID: CM-Funktion_EFO_5_100						
SELECT (DF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden DF.

3.1655.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1656 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_101)

3.1656.1 Informationen

ID	TC_Funktion_EFO_5_101
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CREATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1656.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1656.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1656.4 APDU-Kommandos

ID: CM-Funktion_EFO_5_101						
CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1656.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1657 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_102)

3.1657.1 Informationen

ID	TC_Funktion_EFO_5_102
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CREATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1657.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1657.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1657.4 APDU-Kommandos

ID: CM-Funktion_EFO_5_102						
CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1657.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1658 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_103)

3.1658.1 Informationen

ID	TC_Funktion_EFO_5_103
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CREATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1658.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1658.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1658.4 APDU-Kommandos

ID: CM-Funktion_EFO_5_103 CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1658.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1659 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_104)

3.1659.1 Informationen

ID	TC_Funktion_EFO_5_104
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DELETE FILE'

	und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1659.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1659.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1659.4 APDU-Kommandos

ID: CM-Funktion_EFO_5_104						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1659.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1660 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_105)

3.1660.1 Informationen

ID	TC_Funktion_EFO_5_105
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen

	genügen. Die Durchführung erfolgt für das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1660.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1660.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1660.4 APDU-Kommandos

ID: CM-Funktion_EFO_5_105						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1660.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1661 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_106)

3.1661.1 Informationen

ID	TC_Funktion_EFO_5_106
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und

	"Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DELETE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1661.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1661.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1661.4 APDU-Kommandos

ID: CM-Funktion_EFO_5_106						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1661.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1662 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_107)

3.1662.1 Informationen

ID	TC_Funktion_EFO_5_107
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten DF, ob die Karten- und Dateisystem-Management-

	Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'ACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1662.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1662.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1662.4 APDU-Kommandos

ID: CM-Funktion_EFO_5_107						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1662.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1663 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_108)

3.1663.1 Informationen

ID	TC_Funktion_EFO_5_108
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im

	MF angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1663.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1663.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1663.4 APDU-Kommandos

ID: CM-Funktion_EFO_5_108						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1663.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1664 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_109)

3.1664.1 Informationen

ID	TC_Funktion_EFO_5_109
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und

	Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1664.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1664.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1664.4 APDU-Kommandos

ID: CM-Funktion_EFO_5_109							
ACTIVATE FILE							
CLA	INS	P1	P2	Lc	Data	Le	
00	44	00	00	--	--	--	

3.1664.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1665 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_110)

3.1665.1 Informationen

ID	TC_Funktion_EFO_5_110

Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1665.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1665.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1665.4 APDU-Kommandos

ID: CM-Funktion_EFO_5_110						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1665.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1666 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_111)

3.1666.1 Informationen

ID	TC_Funktion_EFO_5_111

Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1666.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1666.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1666.4 APDU-Kommandos

ID: CM-Funktion_EFO_5_111						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1666.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1667 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_112)

3.1667.1 Informationen

ID	TC_Funktion_EFO_5_112

Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1667.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1667.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1667.4 APDU-Kommandos

ID: CM-Funktion_EFO_5_112						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1667.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1668 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_113)

3.1668.1 Informationen

ID	TC_Funktion_EFO_5_113

Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'TERMINATE DF' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1668.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1668.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1668.4 APDU-Kommandos

ID: CM-Funktion_EFO_5_113						
TERMINATE DF						
CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

3.1668.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1669 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_114)

3.1669.1 Informationen

ID	TC_Funktion_EFO_5_114

Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'TERMINATE DF' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1669.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1669.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1669.4 APDU-Kommandos

ID: CM-Funktion_EFO_5_114						
TERMINATE DF						
CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

3.1669.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1670 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_5_115)

3.1670.1 Informationen

ID	TC_Funktion_EFO_5_115

Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'TERMINATE DF' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1670.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1670.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1670.4 APDU-Kommandos

ID: CM-Funktion_EFO_5_115						
TERMINATE DF						
CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

3.1670.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1671 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_116)

3.1671.1 Informationen

ID	TC_Funktion_EFO_6_116

Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'SELECT EF' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1671.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1671.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1671.4 APDU-Kommandos

ID: CM-Funktion_EFO_6_116						
SELECT (EF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	02	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

3.1671.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1672 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_117)

3.1672.1 Informationen

ID	TC_Funktion_EFO_6_117
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CREATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1672.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1672.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1672.4 APDU-Kommandos

ID: CM-Funktion_EFO_6_117 CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1672.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1673 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_118)

3.1673.1 Informationen

ID	TC_Funktion_EFO_6_118
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CREATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1673.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1673.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1673.4 APDU-Kommandos

ID: CM-Funktion_EFO_6_118 CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1673.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1674 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_119)

3.1674.1 Informationen

ID	TC_Funktion_EFO_6_119
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CREATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1674.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1674.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1674.4 APDU-Kommandos

ID: CM-Funktion_EFO_6_119
CREATE FILE

CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1674.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1675 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_120)

3.1675.1 Informationen

ID	TC_Funktion_EFO_6_120
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DELETE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1675.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1675.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1675.4 APDU-Kommandos

ID: CM-Funktion_EFO_6_120						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1675.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1676 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_121)

3.1676.1 Informationen

ID	TC_Funktion_EFO_6_121
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1676.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1676.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1676.4 APDU-Kommandos

ID: CM-Funktion_EFO_6_121						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1676.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1677 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_122)

3.1677.1 Informationen

ID	TC_Funktion_EFO_6_122
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DELETE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1677.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1677.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1677.4 APDU-Kommandos

ID: CM-Funktion_EFO_6_122						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1677.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1678 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_123)

3.1678.1 Informationen

ID	TC_Funktion_EFO_6_123
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'ACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1678.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1678.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1678.4 APDU-Kommandos

ID: CM-Funktion_EFO_6_123						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1678.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1679 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_124)

3.1679.1 Informationen

ID	TC_Funktion_EFO_6_124
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1679.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1679.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1679.4 APDU-Kommandos

ID: CM-Funktion_EFO_6_124						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1679.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1680 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_125)

3.1680.1 Informationen

ID	TC_Funktion_EFO_6_125
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1680.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1680.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1680.4 APDU-Kommandos

ID: CM-Funktion_EFO_6_125						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1680.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1681 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_126)

3.1681.1 Informationen

ID	TC_Funktion_EFO_6_126
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1681.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1681.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1681.4 APDU-Kommandos

ID: CM-Funktion_EFO_6_126						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1681.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1682 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_127)

3.1682.1 Informationen

ID	TC_Funktion_EFO_6_127
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1682.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1682.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1682.4 APDU-Kommandos

ID: CM-Funktion_EFO_6_127						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1682.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1683 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_128)

3.1683.1 Informationen

ID	TC_Funktion_EFO_6_128
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1683.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1683.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1683.4 APDU-Kommandos

ID: CM-Funktion_EFO_6_128						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1683.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1684 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_129)

3.1684.1 Informationen

ID	TC_Funktion_EFO_6_129
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'TERMINATE DF' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1684.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1684.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1684.4 APDU-Kommandos

ID: CM-Funktion_EFO_6_129						
TERMINATE DF						
CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

3.1684.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1685 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_130)

3.1685.1 Informationen

ID	TC_Funktion_EFO_6_130
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'TERMINATE DF' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1685.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1685.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1685.4 APDU-Kommandos

ID: CM-Funktion_EFO_6_130						
TERMINATE DF						
CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

3.1685.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1686 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_6_131)

3.1686.1 Informationen

ID	TC_Funktion_EFO_6_131
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im MF korrekt gesetzt sind. Der Testfall prüft anhand von neu im MF angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'TERMINATE DF' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1686.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1686.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1686.4 APDU-Kommandos

ID: CM-Funktion_EFO_6_131						
TERMINATE DF						
CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

3.1686.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1687 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_1)

3.1687.1 Informationen

ID	TC_Funktion_EFO_7_1
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CREATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1687.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1687.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1687.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_1						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1687.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1688 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_2)

3.1688.1 Informationen

ID	TC_Funktion_EFO_7_2
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CREATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1688.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1688.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1688.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_2						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1688.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1689 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_3)

3.1689.1 Informationen

ID	TC_Funktion_EFO_7_3
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CREATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1689.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1689.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1689.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_3						
CREATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	81	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName || 96-L96-KeyUsageCounterInit || A1-00 bzw. A2-00 || 7B-L7B- A4-LA4-(80-L80-CryptoID) (|| A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (|| B6-LB6-(80-L80-CryptoID))'

3.1689.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1690 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_4)

3.1690.1 Informationen

ID	TC_Funktion_EFO_7_4
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DELETE KEY'

	und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1690.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1690.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1690.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_4						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1690.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1691 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_5)

3.1691.1 Informationen

ID	TC_Funktion_EFO_7_5

Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DELETE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1691.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1691.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1691.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_5						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1691.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1692 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_6)

3.1692.1 Informationen

ID	TC_Funktion_EFO_7_6
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DELETE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1692.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1692.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1692.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_6						
DELETE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1692.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1693 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_7)

3.1693.1 Informationen

ID	TC_Funktion_EFO_7_7
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'ACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1693.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1693.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1693.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_7						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1693.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1694 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_8)

3.1694.1 Informationen

ID	TC_Funktion_EFO_7_8
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1694.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1694.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1694.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_8 ACTIVATE KEY

CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1694.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1695 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_9)

3.1695.1 Informationen

ID	TC_Funktion_EFO_7_9
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'ACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1695.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1695.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1695.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_9						
ACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	44	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1695.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1696 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_10)

3.1696.1 Informationen

ID	TC_Funktion_EFO_7_10
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DEACTIVATE KEY' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1696.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1696.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1696.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_10 DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1696.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1697 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_11)

3.1697.1 Informationen

ID	TC_Funktion_EFO_7_11
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1697.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1697.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1697.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_11						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1697.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1698 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_12)

3.1698.1 Informationen

ID	TC_Funktion_EFO_7_12
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen

	genügen. Die Durchführung erfolgt für das Kommando 'DEACTIVATE KEY' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1698.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1698.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1698.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_12						
DEACTIVATE KEY						
CLA	INS	P1	P2	Lc	Data	Le
00	04	21	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

3.1698.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1699 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_13)

3.1699.1 Informationen

ID	TC_Funktion_EFO_7_13

Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselgenerierung mit Export des Public Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1699.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1699.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1699.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_13						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1699.5 Erwartete Ergebnisse

ID	Beschreibung

RS-6982	Das Testsystem antwortet mit '69 82'.

3.1700 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_14)

3.1700.1 Informationen

ID	TC_Funktion_EFO_7_14
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselgenerierung mit Export des Public Key)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1700.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1700.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1700.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_14						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT):

'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1700.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1701 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_15)

3.1701.1 Informationen

ID	TC_Funktion_EFO_7_15
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselgenerierung mit Export des Public Key)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1701.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1701.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1701.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_15

GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung mit Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	82	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1701.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1702 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_16)

3.1702.1 Informationen

ID	TC_Funktion_EFO_7_16
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselgenerierung ohne Export des Public Key)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1702.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1702.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1702.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_16						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1702.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1703 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_17)

3.1703.1 Informationen

ID	TC_Funktion_EFO_7_17
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselgenerierung ohne Export des Public Key)' und den Sicherheitszustand PACE.

Klassifizierung	Fehlerfall-Test

3.1703.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1703.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1703.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_17						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1703.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1704 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_18)

3.1704.1 Informationen

ID	TC_Funktion_EFO_7_18

Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERATE ASYMMETRIC KEY PAIR (Schlüsselgenerierung ohne Export des Public Key)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1704.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1704.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1704.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_18						
GENERATE ASYMMETRIC KEY PAIR (Schlüsselerzeugung ohne Export des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	86	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) || 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'

3.1704.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1705 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_19)

3.1705.1 Informationen

ID	TC_Funktion_EFO_7_19
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERATE ASYMMETRIC KEY PAIR (nur Schlüsselexport, ohne Schlüsselgenerierung)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1705.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1705.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1705.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_19						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1705.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1706 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_20)

3.1706.1 Informationen

ID	TC_Funktion_EFO_7_20
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERATE ASYMMETRIC KEY PAIR (nur Schlüsselexport, ohne Schlüsselgenerierung)' und den Sicherheitszustand PACE.
Klassifizierung	Gutfall-Test

3.1706.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1706.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1706.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_20						
GENERATE ASYMMETRIC KEY AIR (Ausgabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	47	83	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1706.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1707 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_21)

3.1707.1 Informationen

ID	TC_Funktion_EFO_7_21
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1707.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1707.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1707.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_21
PSO COMPUTE DIGITAL SIGNATURE

CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1707.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1708 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_22)

3.1708.1 Informationen

ID	TC_Funktion_EFO_7_22
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'PSO COMPUTE DIGITAL SIGNATURE' und den Sicherheitszustand PACE.
Klassifizierung	Gutfall-Test

3.1708.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1708.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1708.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_22 PSO COMPUTE DIGITAL SIGNATURE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	9e	9a	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu signierende Daten als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1708.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1709 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_23)

3.1709.1 Informationen

ID	TC_Funktion_EFO_7_23
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'PSO VERIFY DIGITAL SIGNATURE (Variante ohne Übergabe des Public-Key im Kommando)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1709.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1709.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1709.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_23						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1709.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1710 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_24)

3.1710.1 Informationen

ID	TC_Funktion_EFO_7_24
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'PSO VERIFY DIGITAL SIGNATURE (Variante ohne Übergabe des Public-Key im Kommando)' und den Sicherheitszustand PACE.
Klassifizierung	Gutfall-Test

3.1710.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1710.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1710.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_24						
PSO VERIFY DIGITAL SIGNATURE (ohne Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash || 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge)

3.1710.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1711 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_25)

3.1711.1 Informationen

ID	TC_Funktion_EFO_7_25
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'PSO VERIFY

	DIGITAL SIGNATURE (Variante mit Übergabe des Public Key im Kommando)' und den Sicherheitszustand PACE oder ohne Sicherheitszustand, abhängig vom CLA-Byte des Kommandos.
Klassifizierung	

3.1711.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1711.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1711.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_25						
PSO VERIFY DIGITAL SIGNATURE (mit Übergabe des Public-Key)						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	a8	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID || 90-L90-Hash || 9C-L9C-PubKey || 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R || S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.

3.1711.5 Erwartete Ergebnisse

ID	Beschreibung
RS-E718	69 82 oder 90 00, abhängig vom CLA-Byte des Kommandos

3.1712 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_26)

3.1712.1 Informationen

ID	TC_Funktion_EFO_7_26
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'PSO VERIFY CERTIFICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1712.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1712.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1712.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_26						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1712.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1713 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_27)

3.1713.1 Informationen

ID	TC_Funktion_EFO_7_27
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1713.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1713.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1713.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_27						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1713.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1714 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_28)

3.1714.1 Informationen

ID	TC_Funktion_EFO_7_28
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'PSO VERIFY CERTIFICATE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1714.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1714.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1714.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_28						
PSO VERIFY CERTIFICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	2a	00	be	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody || 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R || S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

3.1714.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1715 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_29)

3.1715.1 Informationen

ID	TC_Funktion_EFO_7_29
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1715.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1715.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1715.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_29						
GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1715.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1716 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_30)

3.1716.1 Informationen

ID	TC_Funktion_EFO_7_30
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und

	"Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1716.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1716.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1716.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_30 GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1716.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1717 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_31)

3.1717.1 Informationen

ID	TC_Funktion_EFO_7_31
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERAL AUTHENTICATE (ECKA-EG)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1717.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1717.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1717.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_31 GENERAL AUTHENTICATE (ECKA-EG)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der Elliptischen Kurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator

sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).

3.1717.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1718 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_32)

3.1718.1 Informationen

ID	TC_Funktion_EFO_7_32
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1718.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1718.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1718.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_32						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le

00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1718.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1719 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_33)

3.1719.1 Informationen

ID	TC_Funktion_EFO_7_33
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1719.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1719.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1719.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_33						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1719.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1720 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_34)

3.1720.1 Informationen

ID	TC_Funktion_EFO_7_34
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERAL AUTHENTICATE (ECKA-DH)' und den Sicherheitszustand PACE + AUTH.

Klassifizierung	Gutfall-Test

3.1720.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1720.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1720.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_34						
GENERAL AUTHENTICATE (ECKA-DH)						
CLA	INS	P1	P2	Lc	Data	Le
00	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve || (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

3.1720.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1721 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_35)

3.1721.1 Informationen

ID	TC_Funktion_EFO_7_35
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GENERAL AUTHENTICATE (PACE)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1721.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1721.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1721.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_35 GENERAL AUTHENTICATE (PACE)						
CLA	INS	P1	P2	Lc	Data	Le
XX	86	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW)

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1721.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1722 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_36)

3.1722.1 Informationen

ID	TC_Funktion_EFO_7_36
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'EXTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1722.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1722.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1722.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_36 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1722.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1723 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_37)

3.1723.1 Informationen

ID	TC_Funktion_EFO_7_37
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'EXTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Gutfall-Test

3.1723.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1723.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1723.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_37 EXTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	82	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält den Authentisierungstoken als Oktett-String.

3.1723.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1724 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_38)

3.1724.1 Informationen

ID	TC_Funktion_EFO_7_38
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'INTERNAL AUTHENTICATE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1724.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1724.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1724.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_38 INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1724.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1725 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_7_39)

3.1725.1 Informationen

ID	TC_Funktion_EFO_7_39
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten Schlüsseln, ob die Key-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'INTERNAL AUTHENTICATE' und den Sicherheitszustand PACE.
Klassifizierung	Gutfall-Test

3.1725.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1725.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1725.4 APDU-Kommandos

ID: CM-Funktion_EFO_7_39						
INTERNAL AUTHENTICATE						
CLA	INS	P1	P2	Lc	Data	Le
00	88	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält das Token als Oktett-String.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1725.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1726 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_8_40)

3.1726.1 Informationen

ID	TC_Funktion_EFO_8_40
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten PIN-Objekten, ob die PIN-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CHANGE REFERENCE DATA (Variante Wechseln einer PIN mit der LCSI (PIN-LifeCycleStatus) initialisation)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1726.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1726.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1726.4 APDU-Kommandos

ID: CM-Funktion_EFO_8_40
CHANGE REFERENCE DATA (Wechseln einer PIN)

CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

3.1726.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1727 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_8_41)

3.1727.1 Informationen

ID	TC_Funktion_EFO_8_41
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten PIN-Objekten, ob die PIN-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CHANGE REFERENCE DATA (Variante Wechseln einer PIN mit der LCS (PIN-LifeCycleStatus) initialisation)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1727.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1727.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1727.4 APDU-Kommandos

ID: CM-Funktion_EFO_8_41						
CHANGE REFERENCE DATA (Wechseln einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

3.1727.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1728 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_8_42)

3.1728.1 Informationen

ID	TC_Funktion_EFO_8_42
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten PIN-Objekten, ob die PIN-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CHANGE REFERENCE DATA (Variante Wechseln einer PIN mit der LCS (PIN-LifeCycleStatus) initialisation)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1728.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1728.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1728.4 APDU-Kommandos

ID: CM-Funktion_EFO_8_42						
CHANGE REFERENCE DATA (Wechseln einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

3.1728.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1729 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_8_43)

3.1729.1 Informationen

ID	TC_Funktion_EFO_8_43
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten PIN-Objekten, ob die PIN-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CHANGE REFERENCE DATA (Variante Wechseln einer PIN mit der LCS (PIN-LifeCycleStatus) operational state - activated)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1729.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1729.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1729.4 APDU-Kommandos

ID: CM-Funktion_EFO_8_43 CHANGE REFERENCE DATA (Wechseln einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

3.1729.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1730 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_8_44)

3.1730.1 Informationen

ID	TC_Funktion_EFO_8_44
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten PIN-Objekten, ob die PIN-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CHANGE REFERENCE DATA (Variante Wechseln einer PIN mit der LCSI (PIN-

	LifeCycleStatus) operational state - activated)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1730.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1730.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1730.4 APDU-Kommandos

ID: CM-Funktion_EFO_8_44 CHANGE REFERENCE DATA (Wechseln einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

3.1730.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1731 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_8_45)

3.1731.1 Informationen

ID	TC_Funktion_EFO_8_45
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und

	Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten PIN-Objekten, ob die PIN-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CHANGE REFERENCE DATA (Variante Wechseln einer PIN mit der LCS (PIN-LifeCycleStatus) operational state - activated)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1731.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1731.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1731.4 APDU-Kommandos

ID: CM-Funktion_EFO_8_45						
CHANGE REFERENCE DATA (Wechseln einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

3.1731.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1732 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_8_46)

3.1732.1 Informationen

ID	TC_Funktion_EFO_8_46
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten PIN-Objekten, ob die PIN-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CHANGE REFERENCE DATA (Variante Wechseln einer PIN)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1732.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1732.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1732.4 APDU-Kommandos

ID: CM-Funktion_EFO_8_46						
CHANGE REFERENCE DATA (Wechseln einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

3.1732.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1733 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_8_47)

3.1733.1 Informationen

ID	TC_Funktion_EFO_8_47
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten PIN-Objekten, ob die PIN-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CHANGE REFERENCE DATA (Variante Wechseln einer PIN)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1733.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1733.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1733.4 APDU-Kommandos

ID: CM-Funktion_EFO_8_47						
CHANGE REFERENCE DATA (Wechseln einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

3.1733.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1734 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_8_48)

3.1734.1 Informationen

ID	TC_Funktion_EFO_8_48
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten PIN-Objekten, ob die PIN-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CHANGE REFERENCE DATA (Variante Wechseln einer PIN)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1734.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1734.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1734.4 APDU-Kommandos

ID: CM-Funktion_EFO_8_48
CHANGE REFERENCE DATA (Wechseln einer PIN)

CLA	INS	P1	P2	Lc	Data	Le
00	24	00	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält 'Alte PIN' || 'Neue PIN'.

3.1734.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1735 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_8_49)

3.1735.1 Informationen

ID	TC_Funktion_EFO_8_49
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten PIN-Objekten, ob die PIN-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CHANGE REFERENCE DATA (Variante Setzen einer PIN)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1735.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1735.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1735.4 APDU-Kommandos

ID: CM-Funktion_EFO_8_49						
CHANGE REFERENCE DATA (Setzen einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	01	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die neue PIN.

3.1735.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1736 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_8_50)

3.1736.1 Informationen

ID	TC_Funktion_EFO_8_50
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten PIN-Objekten, ob die PIN-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CHANGE REFERENCE DATA (Variante Setzen einer PIN)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1736.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1736.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1736.4 APDU-Kommandos

ID: CM-Funktion_EFO_8_50						
CHANGE REFERENCE DATA (Setzen einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	01	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die neue PIN.

3.1736.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1737 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_8_51)

3.1737.1 Informationen

ID	TC_Funktion_EFO_8_51
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten PIN-Objekten, ob die PIN-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CHANGE REFERENCE DATA (Variante Setzen einer PIN)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1737.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1737.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1737.4 APDU-Kommandos

ID: CM-Funktion_EFO_8_51 CHANGE REFERENCE DATA (Setzen einer PIN)						
CLA	INS	P1	P2	Lc	Data	Le
00	24	01	XX	LL	XX...XX	--

'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die neue PIN.

3.1737.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1738 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_52)

3.1738.1 Informationen

ID	TC_Funktion_EFO_9_52
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ BINARY (für nicht initiale EF mit LCSi initialisation)'

	und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1738.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1738.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1738.4 APDU-Kommandos

ID: CM-Funktion_EFO_9_52 READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1738.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1739 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_53)

3.1739.1 Informationen

ID	TC_Funktion_EFO_9_53
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von

	neu im DF.SMGW angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ BINARY (für nicht initiale EF mit LCSi operational state - activated)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1739.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1739.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1739.4 APDU-Kommandos

ID: CM-Funktion_EFO_9_53						
READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1739.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1740 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_54)

3.1740.1 Informationen

ID	TC_Funktion_EFO_9_54
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ BINARY (für nicht initiale EF mit LCSi operational state - deactivated)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1740.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1740.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1740.4 APDU-Kommandos

ID: CM-Funktion_EFO_9_54						
READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1740.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1741 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_55)

3.1741.1 Informationen

ID	TC_Funktion_EFO_9_55
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ BINARY (für nicht initiale EF mit LCSi operational state - deactivated)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1741.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1741.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1741.4 APDU-Kommandos

ID: CM-Funktion_EFO_9_55						
READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1741.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1742 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_56)

3.1742.1 Informationen

ID	TC_Funktion_EFO_9_56
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ BINARY (für nicht initiale EF mit LCSI operational state - deactivated)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1742.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1742.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1742.4 APDU-Kommandos

ID: CM-Funktion_EFO_9_56
READ BINARY (ohne SFI)

CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1742.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1743 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_57)

3.1743.1 Informationen

ID	TC_Funktion_EFO_9_57
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ BINARY (für nicht initiale EF mit LCS terminated)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1743.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1743.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1743.4 APDU-Kommandos

ID: CM-Funktion_EFO_9_57						
READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1743.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1744 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_58)

3.1744.1 Informationen

ID	TC_Funktion_EFO_9_58
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ BINARY (für nicht initiale EF mit LCS terminated)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1744.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1744.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1744.4 APDU-Kommandos

ID: CM-Funktion_EFO_9_58 READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1744.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1745 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_59)

3.1745.1 Informationen

ID	TC_Funktion_EFO_9_59
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ BINARY (für nicht initiale EF mit LCSI terminated)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1745.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1745.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1745.4 APDU-Kommandos

ID: CM-Funktion_EFO_9_59						
READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1745.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1746 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_60)

3.1746.1 Informationen

ID	TC_Funktion_EFO_9_60
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE BINARY (für nicht initiale EF mit LCS

	initialisation)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1746.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1746.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1746.4 APDU-Kommandos

ID: CM-Funktion_EFO_9_60 READ BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b0	XX	XX	--	--	XX

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1746.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1747 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_61)

3.1747.1 Informationen

ID	TC_Funktion_EFO_9_61
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von

	neu im DF.SMGW angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE BINARY (für nicht initiale EF mit LCSI operational state - activated)' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1747.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1747.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1747.4 APDU-Kommandos

ID: CM-Funktion_EFO_9_61 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1747.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1748 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_62)

3.1748.1 Informationen

ID	TC_Funktion_EFO_9_62
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE BINARY (für nicht initiale EF mit LCSI operational state - deactivated)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1748.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1748.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1748.4 APDU-Kommandos

ID: CM-Funktion_EFO_9_62 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1748.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1749 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_63)

3.1749.1 Informationen

ID	TC_Funktion_EFO_9_63
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE BINARY (für nicht initiale EF mit LCSI operational state - deactivated)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1749.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1749.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1749.4 APDU-Kommandos

ID: CM-Funktion_EFO_9_63 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1749.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1750 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_64)

3.1750.1 Informationen

ID	TC_Funktion_EFO_9_64
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE BINARY (für nicht initiale EF mit LCSI operational state - deactivated)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1750.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1750.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1750.4 APDU-Kommandos

ID: CM-Funktion_EFO_9_64

UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1750.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1751 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_65)

3.1751.1 Informationen

ID	TC_Funktion_EFO_9_65
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE BINARY (für nicht initiale EF mit LCSI terminated)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1751.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1751.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1751.4 APDU-Kommandos

ID: CM-Funktion_EFO_9_65 UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1751.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1752 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_66)

3.1752.1 Informationen

ID	TC_Funktion_EFO_9_66
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE BINARY (für nicht initiale EF mit LCSI terminated)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1752.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1752.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1752.4 APDU-Kommandos

ID: CM-Funktion_EFO_9_66						
UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1752.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1753 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_9_67)

3.1753.1 Informationen

ID	TC_Funktion_EFO_9_67
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten transparenten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE BINARY (für nicht initiale EF mit LCSI terminated)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1753.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1753.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1753.4 APDU-Kommandos

ID: CM-Funktion_EFO_9_67						
UPDATE BINARY (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	d6	XX	XX	LL	XX...XX	--

'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.

'P2' enthält den Offset mod 256.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1753.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1754 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_68)

3.1754.1 Informationen

ID	TC_Funktion_EFO_10_68
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung

	des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ RECORD (für nicht initiale record-orientierte EF mit LCSI initialisation)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1754.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1754.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1754.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_68						
READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1754.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1755 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_69)

3.1755.1 Informationen

ID	TC_Funktion_EFO_10_69

Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ RECORD (für nicht initiale record-orientierte EF mit LCSI initialisation)' und den Sicherheitszustand PACE.
Klassifizierung	Gutfall-Test

3.1755.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1755.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1755.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_69						
READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1755.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1756 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_70)

3.1756.1 Informationen

ID	TC_Funktion_EFO_10_70
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ RECORD (für nicht initiale record-orientierte EF mit LCSI operational state - activated)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1756.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1756.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1756.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_70 READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1756.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1757 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_71)

3.1757.1 Informationen

ID	TC_Funktion_EFO_10_71
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ RECORD (für nicht initiale record-orientierte EF mit LCSI operational state - activated)' und den Sicherheitszustand PACE.
Klassifizierung	Gutfall-Test

3.1757.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1757.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1757.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_71 READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1757.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1758 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_72)

3.1758.1 Informationen

ID	TC_Funktion_EFO_10_72
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ RECORD (für nicht initiale record-orientierte EF mit LCSI operation state - deactivated)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1758.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1758.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1758.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_72 READ RECORD (ohne SFI)

CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1758.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1759 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_73)

3.1759.1 Informationen

ID	TC_Funktion_EFO_10_73
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ RECORD (für nicht initiale record-orientierte EF mit LCSi operation state - deactivated)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1759.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1759.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1759.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_73						
READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1759.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1760 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_74)

3.1760.1 Informationen

ID	TC_Funktion_EFO_10_74
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ RECORD (für nicht initiale record-orientierte EF mit LCSI operation state - deactivated)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1760.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1760.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1760.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_74						
READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1760.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1761 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_75)

3.1761.1 Informationen

ID	TC_Funktion_EFO_10_75
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ RECORD (für nicht initiale record-orientierte EF mit LCSI terminated)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1761.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1761.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1761.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_75						
READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1761.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1762 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_76)

3.1762.1 Informationen

ID	TC_Funktion_EFO_10_76
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ RECORD (für nicht initiale record-orientierte EF mit

	LCSI terminated)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1762.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1762.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1762.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_76 READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1762.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1763 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_77)

3.1763.1 Informationen

ID	TC_Funktion_EFO_10_77
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von

	neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'READ RECORD (für nicht initiale record-orientierte EF mit LCSI terminated)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1763.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1763.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1763.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_77						
READ RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	b2	XX	04	--	--	XX

'P1' enthält die Record-Number.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1763.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1764 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_78)

3.1764.1 Informationen

ID	TC_Funktion_EFO_10_78
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE RECORD (für nicht initiale record-orientierte EF mit LCSi initialisation)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1764.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1764.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1764.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_78 UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1764.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1765 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_79)

3.1765.1 Informationen

ID	TC_Funktion_EFO_10_79
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE RECORD (für nicht initiale record-orientierte EF mit LCSi initialisation)' und den Sicherheitszustand PACE.
Klassifizierung	Gutfall-Test

3.1765.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1765.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1765.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_79 UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1765.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1766 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_80)

3.1766.1 Informationen

ID	TC_Funktion_EFO_10_80
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE RECORD (für nicht initiale record-orientierte EF mit LCSi operational state - activated)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1766.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1766.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1766.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_80

UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1766.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1767 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_81)

3.1767.1 Informationen

ID	TC_Funktion_EFO_10_81
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE RECORD (für nicht initiale record-orientierte EF mit LCSI operational state - activated)' und den Sicherheitszustand PACE.
Klassifizierung	Gutfall-Test

3.1767.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1767.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1767.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_81 UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1767.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1768 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_82)

3.1768.1 Informationen

ID	TC_Funktion_EFO_10_82
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE RECORD (für nicht initiale record-orientierte EF mit LCSI operational state - deactivated)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1768.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1768.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1768.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_82 UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1768.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1769 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_83)

3.1769.1 Informationen

ID	TC_Funktion_EFO_10_83
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE RECORD (für nicht initiale record-orientierte EF mit LCSI operational state - deactivated)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1769.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1769.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1769.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_83						
UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1769.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1770 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_84)

3.1770.1 Informationen

ID	TC_Funktion_EFO_10_84
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das

	Kommando 'UPDATE RECORD (für nicht initiale record-orientierte EF mit LCSI operational state - deactivated)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1770.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1770.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1770.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_84 UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1770.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1771 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_85)

3.1771.1 Informationen

ID	TC_Funktion_EFO_10_85
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE RECORD (für nicht initiale record-orientierte EF mit LCSi terminated)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1771.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1771.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1771.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_85 UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1771.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1772 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_86)

3.1772.1 Informationen

ID	TC_Funktion_EFO_10_86
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE RECORD (für nicht initiale record-orientierte EF mit LCSi terminated)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1772.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1772.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1772.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_86 UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1772.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1773 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_87)

3.1773.1 Informationen

ID	TC_Funktion_EFO_10_87
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'UPDATE RECORD (für nicht initiale record-orientierte EF mit LCSi terminated)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1773.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1773.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1773.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_87

UPDATE RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	dc	XX	04	LL	XX...XX	--

'P1' enthält die Record-Number.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden neuen Daten.

3.1773.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1774 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_88)

3.1774.1 Informationen

ID	TC_Funktion_EFO_10_88
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'APPEND RECORD (für nicht initiale record-orientierte EF mit LCSi initialisation, sofern implementiert)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1774.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1774.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1774.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_88 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1774.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1775 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_89)

3.1775.1 Informationen

ID	TC_Funktion_EFO_10_89
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'APPEND RECORD (für nicht initiale record-orientierte EF mit LCSi initialisation, sofern implementiert)' und den Sicherheitszustand PACE.
Klassifizierung	Gutfall-Test

3.1775.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1775.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1775.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_89						
APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1775.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1776 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_90)

3.1776.1 Informationen

ID	TC_Funktion_EFO_10_90
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'APPEND RECORD (für nicht initiale record-orientierte EF mit LCSi operational state - activated, sofern implementiert)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1776.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1776.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1776.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_90 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1776.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1777 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_91)

3.1777.1 Informationen

ID	TC_Funktion_EFO_10_91
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'APPEND RECORD (für nicht initiale record-orientierte EF

	mit LCSI operational state - activated, sofern implementiert)' und den Sicherheitszustand PACE.
Klassifizierung	Gutfall-Test

3.1777.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1777.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1777.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_91 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1777.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1778 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_92)

3.1778.1 Informationen

ID	TC_Funktion_EFO_10_92
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und

	Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'APPEND RECORD (für nicht initiale record-orientierte EFoperational state - deactivated, sofern implementiert)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1778.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1778.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1778.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_92 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1778.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1779 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_93)

3.1779.1 Informationen

ID	TC_Funktion_EFO_10_93
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'APPEND RECORD (für nicht initiale record-orientierte EFOperational state - deactivated, sofern implementiert)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1779.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1779.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1779.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_93 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1779.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1780 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_94)

3.1780.1 Informationen

ID	TC_Funktion_EFO_10_94
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'APPEND RECORD (für nicht initiale record-orientierte EFoperational state - deactivated, sofern implementiert)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1780.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1780.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1780.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_94 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le

00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1780.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1781 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_95)

3.1781.1 Informationen

ID	TC_Funktion_EFO_10_95
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'APPEND RECORD (für nicht initiale record-orientierte EF LCSI terminated, sofern implementiert)' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1781.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1781.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1781.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_95						
APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1781.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1782 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_96)

3.1782.1 Informationen

ID	TC_Funktion_EFO_10_96
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'APPEND RECORD (für nicht initiale record-orientierte EF LCSI terminated, sofern implementiert)' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1782.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1782.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1782.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_96 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1782.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1783 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_10_97)

3.1783.1 Informationen

ID	TC_Funktion_EFO_10_97
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten record-orientierten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'APPEND RECORD (für nicht initiale record-orientierte EF LCSI terminated, sofern implementiert)' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Fehlerfall-Test

3.1783.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1783.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1783.4 APDU-Kommandos

ID: CM-Funktion_EFO_10_97 APPEND RECORD (ohne SFI)						
CLA	INS	P1	P2	Lc	Data	Le
00	e2	00	00	LL	XX...XX	--

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die zu schreibenden Record-Daten.

3.1783.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1784 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_98)

3.1784.1 Informationen

ID	TC_Funktion_EFO_11_98
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'SELECT DF' und ohne Sicherheitszustand.

Klassifizierung	Gutfall-Test

3.1784.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1784.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1784.4 APDU-Kommandos

ID: CM-Funktion_EFO_11_98 SELECT (DF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden DF.

3.1784.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1785 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_99)

3.1785.1 Informationen

ID	TC_Funktion_EFO_11_99
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen

	genügen. Die Durchführung erfolgt für das Kommando 'SELECT DF' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1785.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1785.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1785.4 APDU-Kommandos

ID: CM-Funktion_EFO_11_99						
SELECT (DF mittels FID)						
CLA	INS	P1	P2	Lc	Data	Le
00	a4	01	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden DF.

3.1785.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1786 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_100)

3.1786.1 Informationen

ID	TC_Funktion_EFO_11_100
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von

	neu im DF.SMGW angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CREATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1786.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1786.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1786.4 APDU-Kommandos

ID: CM-Funktion_EFO_11_100 CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1786.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1787 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_101)

3.1787.1 Informationen

ID	TC_Funktion_EFO_11_101
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CREATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1787.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1787.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1787.4 APDU-Kommandos

ID: CM-Funktion_EFO_11_101 CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1787.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1788 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_102)

3.1788.1 Informationen

ID	TC_Funktion_EFO_11_102
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CREATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1788.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1788.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1788.4 APDU-Kommandos

ID: CM-Funktion_EFO_11_102 CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1788.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1789 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_103)

3.1789.1 Informationen

ID	TC_Funktion_EFO_11_103
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DELETE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1789.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1789.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1789.4 APDU-Kommandos

ID: CM-Funktion_EFO_11_103
DELETE FILE

CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1789.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1790 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_104)

3.1790.1 Informationen

ID	TC_Funktion_EFO_11_104
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1790.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1790.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1790.4 APDU-Kommandos

ID: CM-Funktion_EFO_11_104
DELETE FILE

CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1790.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1791 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_105)

3.1791.1 Informationen

ID	TC_Funktion_EFO_11_105
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DELETE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1791.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1791.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1791.4 APDU-Kommandos

ID: CM-Funktion_EFO_11_105 DELETE FILE

CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1791.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1792 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_106)

3.1792.1 Informationen

ID	TC_Funktion_EFO_11_106
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'ACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1792.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1792.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1792.4 APDU-Kommandos

ID: CM-Funktion_EFO_11_106
ACTIVATE FILE

CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1792.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1793 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_107)

3.1793.1 Informationen

ID	TC_Funktion_EFO_11_107
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1793.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1793.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1793.4 APDU-Kommandos

ID: CM-Funktion_EFO_11_107 ACTIVATE FILE

CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1793.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1794 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_108)

3.1794.1 Informationen

ID	TC_Funktion_EFO_11_108
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1794.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1794.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1794.4 APDU-Kommandos

ID: CM-Funktion_EFO_11_108
ACTIVATE FILE

CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1794.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1795 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_109)

3.1795.1 Informationen

ID	TC_Funktion_EFO_11_109
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1795.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1795.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1795.4 APDU-Kommandos

ID: CM-Funktion_EFO_11_109 DEACTIVATE FILE

CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1795.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1796 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_110)

3.1796.1 Informationen

ID	TC_Funktion_EFO_11_110
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1796.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1796.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1796.4 APDU-Kommandos

ID: CM-Funktion_EFO_11_110
DEACTIVATE FILE

CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1796.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1797 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_111)

3.1797.1 Informationen

ID	TC_Funktion_EFO_11_111
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1797.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1797.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1797.4 APDU-Kommandos

ID: CM-Funktion_EFO_11_111 DEACTIVATE FILE

CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1797.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1798 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_112)

3.1798.1 Informationen

ID	TC_Funktion_EFO_11_112
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'TERMINATE DF' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1798.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1798.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1798.4 APDU-Kommandos

ID: CM-Funktion_EFO_11_112
TERMINATE DF

CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

3.1798.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1799 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_113)

3.1799.1 Informationen

ID	TC_Funktion_EFO_11_113
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'TERMINATE DF' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1799.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1799.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1799.4 APDU-Kommandos

ID: CM-Funktion_EFO_11_113 TERMINATE DF

CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

3.1799.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1800 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_11_114)

3.1800.1 Informationen

ID	TC_Funktion_EFO_11_114
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten DF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'TERMINATE DF' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1800.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1800.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1800.4 APDU-Kommandos

ID: CM-Funktion_EFO_11_114
TERMINATE DF

CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

3.1800.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1801 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_115)

3.1801.1 Informationen

ID	TC_Funktion_EFO_12_115
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'SELECT EF' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1801.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1801.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1801.4 APDU-Kommandos

ID: CM-Funktion_EFO_12_115 SELECT (EF mittels FID)

CLA	INS	P1	P2	Lc	Data	Le
00	a4	02	0c	02	XX XX	--

'Data' enthält den File-Identifizier des zu selektierenden EF.

3.1801.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1802 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_116)

3.1802.1 Informationen

ID	TC_Funktion_EFO_12_116
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CREATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1802.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1802.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1802.4 APDU-Kommandos

ID: CM-Funktion_EFO_12_116

CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1802.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1803 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_117)

3.1803.1 Informationen

ID	TC_Funktion_EFO_12_117
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CREATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1803.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1803.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1803.4 APDU-Kommandos

ID: CM-Funktion_EFO_12_117						
CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1803.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1804 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_118)

3.1804.1 Informationen

ID	TC_Funktion_EFO_12_118
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'CREATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1804.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1804.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1804.4 APDU-Kommandos

ID: CM-Funktion_EFO_12_118						
CREATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e0	00	00	LL	XX...XX	XX

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File.

'Le' enthält die Anzahl der zu erwartenden Oktette.

3.1804.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1805 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_119)

3.1805.1 Informationen

ID	TC_Funktion_EFO_12_119
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DELETE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1805.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1805.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1805.4 APDU-Kommandos

ID: CM-Funktion_EFO_12_119 DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1805.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1806 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_120)

3.1806.1 Informationen

ID	TC_Funktion_EFO_12_120
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DELETE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1806.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1806.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1806.4 APDU-Kommandos

ID: CM-Funktion_EFO_12_120						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1806.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1807 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_121)

3.1807.1 Informationen

ID	TC_Funktion_EFO_12_121
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DELETE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1807.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1807.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1807.4 APDU-Kommandos

ID: CM-Funktion_EFO_12_121						
DELETE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	e4	00	00	--	--	--

3.1807.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1808 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_122)

3.1808.1 Informationen

ID	TC_Funktion_EFO_12_122
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'ACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1808.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1808.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1808.4 APDU-Kommandos

ID: CM-Funktion_EFO_12_122						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1808.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1809 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_123)

3.1809.1 Informationen

ID	TC_Funktion_EFO_12_123
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1809.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1809.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1809.4 APDU-Kommandos

ID: CM-Funktion_EFO_12_123						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1809.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1810 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_124)

3.1810.1 Informationen

ID	TC_Funktion_EFO_12_124
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'ACTIVATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1810.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1810.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1810.4 APDU-Kommandos

ID: CM-Funktion_EFO_12_124						
ACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	44	00	00	--	--	--

3.1810.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1811 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_125)

3.1811.1 Informationen

ID	TC_Funktion_EFO_12_125
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DEACTIVATE FILE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1811.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1811.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1811.4 APDU-Kommandos

ID: CM-Funktion_EFO_12_125						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1811.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1812 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_126)

3.1812.1 Informationen

ID	TC_Funktion_EFO_12_126
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1812.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1812.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1812.4 APDU-Kommandos

ID: CM-Funktion_EFO_12_126						
DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1812.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1813 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_127)

3.1813.1 Informationen

ID	TC_Funktion_EFO_12_127
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'DEACTIVATE FILE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1813.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1813.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1813.4 APDU-Kommandos

ID: CM-Funktion_EFO_12_127 DEACTIVATE FILE						
CLA	INS	P1	P2	Lc	Data	Le
00	04	00	00	--	--	--

3.1813.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1814 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_128)

3.1814.1 Informationen

ID	TC_Funktion_EFO_12_128
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'TERMINATE DF' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1814.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1814.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1814.4 APDU-Kommandos

ID: CM-Funktion_EFO_12_128						
TERMINATE DF						
CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

3.1814.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1815 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_129)

3.1815.1 Informationen

ID	TC_Funktion_EFO_12_129
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'TERMINATE DF' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1815.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1815.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1815.4 APDU-Kommandos

ID: CM-Funktion_EFO_12_129						
TERMINATE DF						
CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

3.1815.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1816 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_12_130)

3.1816.1 Informationen

ID	TC_Funktion_EFO_12_130
Beschreibung	Es wird getestet, ob Zugriffsregeln von Kommandos auf Dateien und Objekte im DF.SMGW korrekt gesetzt sind. Der Testfall prüft anhand von neu im DF.SMGW angelegten EF, ob die Karten- und Dateisystem-Management-Kommandos in den Phasen "Personalisierung des SMGW" und "Normalbetrieb des SMGW" den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'TERMINATE DF' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1816.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1816.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1816.4 APDU-Kommandos

ID: CM-Funktion_EFO_12_130						
TERMINATE DF						
CLA	INS	P1	P2	Lc	Data	Le
00	e6	00	00	--	--	--

3.1816.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1817 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_13_1)

3.1817.1 Informationen

ID	TC_Funktion_EFO_13_1
Beschreibung	Es wird getestet, ob Zugriffsregeln von speziellen Kommandos korrekt gesetzt sind. Der Testfall prüft, ob die Kommandos zum Management des SE in den Phasen "Personalisierung des SMGW" und "Normalbetrieb" des SMGW den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'MSE SET für externe Authentisierung' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1817.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1817.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1817.4 APDU-Kommandos

ID: CM-Funktion_EFO_13_1						
MSE SET für externe Authentisierung						
CLA	INS	P1	P2	Lc	Data	Le
00	22	81	a4	LL	XX...XX	--

'P1' enthält den jeweiligen Operation-mode in Abhängigkeit von der gewählten Kommandovariante.

'P2' enthält das jeweilige CRT-Tag in Abhängigkeit von der gewählten Kommandovariante.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die jeweiligen Kommandodaten in Abhängigkeit von der gewählten Kommandovariante.

'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.

'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus)
 || '83-L83-Key Reference' (für das Public Key-Objekt)

3.1817.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1818 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_13_2)

3.1818.1 Informationen

ID	TC_Funktion_EFO_13_2
Beschreibung	Es wird getestet, ob Zugriffsregeln von speziellen Kommandos korrekt

	gesetzt sind. Der Testfall prüft, ob die Kommandos zum Management des SE in den Phasen "Personalisierung des SMGW" und "Normalbetrieb" des SMGW den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'MSE RESTORE' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1818.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1818.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1818.4 APDU-Kommandos

ID: CM-Funktion_EFO_13_2						
MSE RESTORE						
CLA	INS	P1	P2	Lc	Data	Le
00	22	f3	XX	--	--	--

'P2' enthält den SEID.

3.1818.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1819 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_14_3)

3.1819.1 Informationen

ID	TC_Funktion_EFO_14_3
Beschreibung	Es wird getestet, ob Zugriffsregeln von speziellen Kommandos korrekt gesetzt sind. Der Testfall prüft, ob die Kommandos zur Zufallsgenerierung

	in den Phasen "Personalisierung des SMGW" und "Normalbetrieb" des SMGW den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'GET CHALLENGE' und den Sicherheitszustand PACE oder ohne Sicherheitszustand, abhängig vom CLA-Byte des Kommandos.
Klassifizierung	

3.1819.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1819.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1819.4 APDU-Kommandos

ID: CM-Funktion_EFO_14_3						
GET CHALLENGE						
CLA	INS	P1	P2	Lc	Data	Le
00	84	XX	00	--	--	XX

'P1' enthält '00': generierte Zufallszahl wird intern gespeichert '01': generierte Zufallszahl wird intern nicht gespeichert.

'Le' enthält die Anzahl der Oktette zu erwartenden Zufallszahl (Hersteller-abhängig und in Abhängigkeit vom Ausgabeformat).

3.1819.5 Erwartete Ergebnisse

ID	Beschreibung
RS-E718	69 82 oder 90 00, abhängig vom CLA-Byte des Kommandos

3.1820 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_15_4)

3.1820.1 Informationen

ID	TC_Funktion_EFO_15_4
Beschreibung	Es wird getestet, ob Zugriffsregeln von speziellen Kommandos korrekt gesetzt sind. Der Testfall prüft, ob die Kommandos zum Management des Life-Cycle-Status in den Phasen "Personalisierung des SMGW" und "Normalbetrieb" des SMGW den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'TERMINATE CARD USAGE' und ohne Sicherheitszustand.
Klassifizierung	Fehlerfall-Test

3.1820.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1820.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1820.4 APDU-Kommandos

ID: CM-Funktion_EFO_15_4						
TERMINATE CARD USAGE						
CLA	INS	P1	P2	Lc	Data	Le
00	fe	00	00	--	--	--

3.1820.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1821 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_15_5)

3.1821.1 Informationen

ID	TC_Funktion_EFO_15_5
Beschreibung	Es wird getestet, ob Zugriffsregeln von speziellen Kommandos korrekt gesetzt sind. Der Testfall prüft, ob die Kommandos zum Management des Life-Cycle-Status in den Phasen "Personalisierung des SMGW" und "Normalbetrieb" des SMGW den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'TERMINATE CARD USAGE' und den Sicherheitszustand PACE.
Klassifizierung	Fehlerfall-Test

3.1821.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1821.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1821.4 APDU-Kommandos

ID: CM-Funktion_EFO_15_5						
TERMINATE CARD USAGE						
CLA	INS	P1	P2	Lc	Data	Le
00	fe	00	00	--	--	--

3.1821.5 Erwartete Ergebnisse

ID	Beschreibung
RS-6982	Das Testsystem antwortet mit '69 82'.

3.1822 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_15_6)

3.1822.1 Informationen

ID	TC_Funktion_EFO_15_6
Beschreibung	Es wird getestet, ob Zugriffsregeln von speziellen Kommandos korrekt gesetzt sind. Der Testfall prüft, ob die Kommandos zum Management des Life-Cycle-Status in den Phasen "Personalisierung des SMGW" und "Normalbetrieb" des SMGW den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'TERMINATE CARD USAGE' und den Sicherheitszustand PACE + AUTH.
Klassifizierung	Gutfall-Test

3.1822.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1822.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1822.4 APDU-Kommandos

ID: CM-Funktion_EFO_15_6						
TERMINATE CARD USAGE						
CLA	INS	P1	P2	Lc	Data	Le
00	fe	00	00	--	--	--

3.1822.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1823 Testfall: Datei- und Objektsystem (TC_Funktion_EFO_16_7)

3.1823.1 Informationen

ID	TC_Funktion_EFO_16_7
Beschreibung	Es wird getestet, ob Zugriffsregeln von speziellen Kommandos korrekt gesetzt sind. Der Testfall prüft, ob die Kommandos zum Management der Applikationsebene in den Phasen "Personalisierung des SMGW" und "Normalbetrieb" des SMGW den definierten Zugriffsbedingungen genügen. Die Durchführung erfolgt für das Kommando 'MANAGE CHANNEL' und ohne Sicherheitszustand.
Klassifizierung	Gutfall-Test

3.1823.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.3.3.3

3.1823.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1823.4 APDU-Kommandos

ID: CM-Funktion_EFO_16_7						
MANAGE CHANNEL						
CLA	INS	P1	P2	Lc	Data	Le
00	70	40	10	--	--	--

3.1823.5 Erwartete Ergebnisse

ID	Beschreibung
RS-9000	Das Testsystem antwortet mit '90 00'.

3.1824 Testfall: Unterstützung CA (TC_Funktion_CAF_1)

3.1824.1 Informationen

ID	TC_Funktion_CAF_1
Beschreibung	Es wird getestet, ob der Umgang mit dem Root-Zertifikat fehlerfrei vonstatten geht. Dieser Testfall prüft, ob das Root-Zertifikat updatefähig ist.
Klassifizierung	Gutfall-Test

3.1824.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 2.1.3.2, 3.2.5

3.1824.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1824.4 APDU-Kommandos

3.1824.5 Erwartete Ergebnisse

ID	Beschreibung
RS-5C16	Das Zertifikat muss updatefähig sein

3.1825 Testfall: Unterstützung CA (TC_Funktion_CAF_2)

3.1825.1 Informationen

ID	TC_Funktion_CAF_2
Beschreibung	Es wird getestet, ob der Umgang mit dem Root-Zertifikat fehlerfrei vonstatten geht. Dieser Testfall prüft, ob genügend Speicherplatz für das Root-Zertifikat vorhanden ist.

Klassifizierung	Gutfall-Test

3.1825.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 2.1.3.2, 3.2.5

3.1825.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1825.4 APDU-Kommandos

3.1825.5 Erwartete Ergebnisse

ID	Beschreibung
RS-B6CF	Es ist genügend Speicherplatz vorhanden sein.

3.1826 Testfall: Protokolle (TC_Funktion_P_1)

3.1826.1 Informationen

ID	TC_Funktion_P_1
Beschreibung	Es wird getestet, ob die eingesetzten Protokolle korrekt funktionieren. Der Testfall prüft mittels durch ein SM-geschütztes Auslesen eines neu angelegten File, ob Secure-Messaging und PACE korrekt umgesetzt sind. Dazu wird ein beliebiges File auf MF-Ebene angelegt und SM-geschützt ausgelesen.
Klassifizierung	Gutfall-Test

3.1826.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Version 1.1, Kapitel 3.5

3.1826.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

n/a

3.1826.4 APDU-Kommandos

3.1826.5 Erwartete Ergebnisse

ID	Beschreibung
RS-67C3	Das File wird korrekt angelegt und ausgelesen

4 Usecase-Tests

4.1 Testfall: VI_01_01

4.1.1 Informationen

ID	VI_01_01
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Auswahl und Setzen des Security Environment (Vor-Personalisierung)
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.1.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.1

4.1.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_01_01-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

4.1.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_01_01-2	Beim Start bzw. Hochfahren des Sicherheitsmoduls ist defaultmäßig das SE mit SEID = 01 gesetzt. Für die Phase „Vor-Personalisierung + Integration von Sicherheitsmodul und GW“ ist explizit das zugehörige SE wie in [TR-03109-2], Kap. 3.3.1, 3.3.3.1 definiert zu setzen.

4.1.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_01_01-3	Es gelten die Zugriffsregeln wie für das zur Phase „Vor-Personalisierung + Integration von Sicherheitsmodul und GW“ zugeordnete Security Environment definiert. Siehe [TR-03109-2], Kap. 3.3.1, 3.3.3.1.

4.1.6 Ablauf

Schritt	Beschreibung						
1	MSE RESTORE (SEID für Phase „Vor-Personalisierung + Integration von Sicherheitsmodul und GW“)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	22	f3	XX	--	--	--
	'P2' enthält den SEID.						

4.1.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.2 Testfall: VI_02_01a

4.2.1 Informationen

ID	VI_02_01a
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Selektieren eines DF/EF (Vor-Personalisierung)
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Rollen	GW, Integrator

4.2.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.2.3

4.2.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_01a-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

4.2.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_01a-2	Die Selektion eines DF/EF per File-ID erfolgt innerhalb des aktuell selektierten DF. Um im Filesystem des Sicherheitsmoduls zu navigieren, ist ggf. eine sukzessive mehrfache Anwendung des Use Case „Selektieren eines DF/EF (Vor-Personalisierung)“ erforderlich.
CN-VI_02_01a-3	Das DF.SMGW kann auch direkt per AID selektiert werden.
CN-VI_02_01a-4	Beim Hochfahren des Sicherheitsmoduls ist automatisch das MF selektiert.

4.2.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.2.6 Ablauf

Schritt	Beschreibung						
1	SELECT: MF (leeres Kommando-Datenfeld)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	a4	00	0c	02	3f 00	--

4.2.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.3 Testfall: VI_02_01b

4.3.1 Informationen

ID	VI_02_01b
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Selektieren eines DF/EF (Vor-Personalisierung)
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.3.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.2.3

4.3.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_01b-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

4.3.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_01b-2	Die Selektion eines DF/EF per File-ID erfolgt innerhalb des aktuell

	selektierten DF/EF. Um im Filesystem des Sicherheitsmoduls zu navigieren, ist ggf. eine sukzessive mehrfache Anwendung des Use Case „Selektieren eines DF/EF (Vor-Personalisierung)“ erforderlich.
CN-VI_02_01b-3	Das DF.SMGW kann auch direkt per AID selektiert werden.
CN-VI_02_01b-4	Beim Hochfahren des Sicherheitsmoduls ist automatisch das MF selektiert.

4.3.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.3.6 Ablauf

Schritt	Beschreibung						
1	SELECT: DF (File-ID des zu selektierenden DF)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	a4	01	0c	02	XX XX	--
	'Data' enthält den File-Identifizier des zu selektierenden DF.						

4.3.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.4 Testfall: VI_02_01c

4.4.1 Informationen

ID	VI_02_01c
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Selektieren eines DF/EF (Vor-Personalisierung)

Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.4.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.2.3

4.4.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_01c-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

4.4.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_01c-2	Die Selektion eines DF/EF per File-ID erfolgt innerhalb des aktuell selektierten DF/EF. Um im Filesystem des Sicherheitsmoduls zu navigieren, ist ggf. eine sukzessive mehrfache Anwendung des Use Case „Selektieren eines DF/EF (Vor-Personalisierung)“ erforderlich.
CN-VI_02_01c-3	Das DF.SMGW kann auch direkt per AID selektiert werden.
CN-VI_02_01c-4	Beim Hochfahren des Sicherheitsmoduls ist automatisch das MF selektiert.

4.4.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.4.6 Ablauf

Schritt	Beschreibung
1	SELECT: DF (File-ID des zu selektierenden EF)

	CLA	INS	P1	P2	Lc	Data	Le
	00	a4	01	0c	02	XX XX	--
	'Data' enthält den File-Identifizier des zu selektierenden DF.						

4.4.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.5 Testfall: VI_02_01d

4.5.1 Informationen

ID	VI_02_01d
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Selektieren eines DF/EF (Vor-Personalisierung)
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.5.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.2.3

4.5.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_01d-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

4.5.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_01d-2	Die Selektion eines DF/EF per File-ID erfolgt innerhalb des aktuell selektierten DF/EF. Um im Filesystem des Sicherheitsmoduls zu navigieren, ist ggf. eine sukzessive mehrfache Anwendung des Use Case „Selektieren eines DF/EF (Vor-Personalisierung)“ erforderlich.
CN-VI_02_01d-3	Das DF.SMGW kann auch direkt per AID selektiert werden.
CN-VI_02_01d-4	Beim Hochfahren des Sicherheitsmoduls ist automatisch das MF selektiert.

4.5.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.5.6 Ablauf

Schritt	Beschreibung						
1	SELECT: DF (AID des DF.SMGW)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	a4	01	0c	02	XX XX	--
	'Data' enthält den File-Identifizier des zu selektierenden DF.						

4.5.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.6 Testfall: VI_02_02a

4.6.1 Informationen

ID	VI_02_02a
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Aktivieren eines DF/EF (Vor-Personalisierung)
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.6.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.2.3

4.6.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_02a-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_02_02a-2	Ausgewähltes FILE ist nicht logisch/physikalisch terminiert

4.6.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_02a-3	Anwendung zur Aktivierung von Ordnern (DF) und Datenfeldern (EF), im vorliegenden Fall insbesondere für das DF.SMGW der SMGW-Applikation, für die transparenten Datenfelder EF.GSCert_TLS, EF.GSCert_SIG und EF.GSCert_ENC für die Gütesiegel-Zertifikate, für die transparenten Datenfelder EF.SMPKIRoot_x für das SM-PKI-Root-Zertifikat sowie für das Record-orientierte Datenfeld EF.GWKeys für die GW-Keys im DF.SMGW.

4.6.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.6.6 Ablauf

Schritt	Beschreibung						
1	SELECT: DF (File-ID des zu aktivierenden DF)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	a4	01	0c	02	XX XX	--
	'Data' enthält den File-Identifizier des zu selektierenden DF.						
2	ACTIVATE FILE						
	CLA	INS	P1	P2	Lc	Data	Le
	00	44	00	00	--	--	--

4.6.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.7 Testfall: VI_02_03

4.7.1 Informationen

ID	VI_02_03
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Löschen eines Key-Objektes (Vor-Personalisierung)
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Rollen	Integrator

4.7.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.2.4

4.7.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_03-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_02_03-2	Zu löschendes Key-Objekt ist deaktiviert. (VI_02_04: Deaktivieren eines Key-Objektes (Vor-Personalisierung))

4.7.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

n/a

4.7.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.7.6 Ablauf

Schritt	Beschreibung						
1	Selektion des DF, in dem das zu löschende Key-Objekt liegt. (VI_02_01: Selektieren eines DF/EF (Vor-Personalisierung))						
2	DELETE KEY (Übergabe der Key Reference des zu löschenden Key-Objektes)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	e4	21	00	LL	XX...XX	--
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-						

	LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST

4.7.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.8 Testfall: VI_02_04

4.8.1 Informationen

ID	VI_02_04
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Deaktivieren eines Key-Objektes (Vor-Personalisierung)
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.8.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.2.4

4.8.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_04-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

4.8.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

n/a

4.8.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.8.6 Ablauf

Schritt	Beschreibung						
1	Selektion des DF, in dem das zu deaktivierende Key-Objekt liegt. (VI_02_01: Selektieren eines DF/EF (Vor-Personalisierung))						
2	DEACTIVATE KEY (Übergabe der Key Reference des zu deaktivierenden Key-Objektes)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	04	21	00	LL	XX...XX	--
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST						

4.8.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.9 Testfall: VI_02_05

4.9.1 Informationen

ID	VI_02_05
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Generierung eines ECC-Schlüsselpaares (Vor-Personalisierung)
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.9.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.2.5

4.9.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_05-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_02_05-2	Key Pair-Objekt, das befüllt werden soll, ist vorhanden. Für die vorläufigen GW-Schlüsselpaare sowie das Integrator-spezifische Import-Schlüsselpaar sind die entsprechenden Key Pair-Objekte bereits im Rahmen der Initialisierung des Sicherheitsmoduls (siehe [TR-03109-2], Kap. 3.1.2) angelegt worden, die dann in diesem Use Case über das Kommando GENERATE ASYMMETRIC KEY PAIR mit Schlüsseldaten gefüllt werden.
CN-VI_02_05-3	Falls ein bereits gefülltes Key Pair-Objekt neu befüllt werden soll: Key-Attribut Key-LifeCycleStatus des Key Pair-Objektes besitzt den Wert „operational state – deactivated“. (VI_02_04: Deaktivieren eines Key-Objektes (Vor-Personalisierung))

4.9.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_05-4	Anwendung für: a) die Generierung der vorläufigen GW-Schlüsselpaare: •.Vorläufiges TLS-Key Pair (GW_WAN_TLS_PRV_PRE, GW_WAN_TLS_PUB_PRE) •.Vorläufiges SIG-Key Pair (GW_WAN_SIG_PRV_PRE, GW_WAN_SIG_PUB_PRE) •.Vorläufiges ENC-Key Pair (GW_WAN_ENC_PRV_PRE, GW_WAN_ENC_PUB_PRE) b) die Generierung des Integrator-spezifischen Import-Schlüssels: •.Import-Key Pair (IMP_PRV, IMP_PUB)
CN-VI_02_05-5	Die Speicherung der in a) genannten vorläufigen GW-Schlüsselpaare erfolgt in den Key Pair-Objekten Key.WAN_TLS_PRE, Key.WAN_SIG_PRE bzw. Key.WAN_ENC_PRE des DF.SMGW. Die Speicherung des in b) genannten Import-Schlüsselpaares erfolgt im Key Pair-Objekt Key.IMP im MF.
CN-VI_02_05-6	Je nach verwendeter Kommando-Variante des Kommandos GENERATE ASYMMETRIC KEY PAIR erfolgt eine Schlüsselgenerierung mit oder ohne Ausgabe des Public Key.

4.9.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_05-7	Das Key-Attribut Key-LifeCycleStatus des Key Pair-Objektes besitzt nach der Schlüsselgenerierung den Wert „operational state – activated“, so dass das Key Pair-Objekt direkt zu seiner Nutzung für Krypto-Operationen bereitsteht.
CN-VI_02_05-8	Sofern im Rahmen der Kommando-Ausführung des Kommandos GENERATE ASYMMETRIC KEY PAIR keine Ausgabe des Public Key-Parts des generierten Schlüsselpaares erfolgt, kann ein späterer Export des Public Key-Parts erfolgen über (VI_02_06: Export des Public Key eines ECC-Schlüsselpaares (Vor-Personalisierung))

4.9.6 Ablauf

Schritt	Beschreibung
1	Selektion des DF, in dem das zu befüllende Key Pair-Objekt liegt. (VI_02_01: Selektieren eines DF/EF (Vor-Personalisierung))
2	GENERATE ASYMMETRIC KEY PAIR: Schlüsselgenerierung ohne Ausgabe des Public Key (Übergabe relevanter Informationen für die Schlüsselgenerierung gemäß

	Kommando-Spezifikation)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	47	86	00	LL	XX...XX	--
'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve'							
3	GENERATE ASYMMETRIC KEY PAIR: Schlüsselgenerierung mit Ausgabe des Public Key (Übergabe relevanter Informationen für die Schlüsselgenerierung gemäß Kommando-Spezifikation)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	47	82	00	LL	XX...XX	XX
'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt. 'Le' enthält die Anzahl der zu erwartenden Oktette.							

4.9.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.10 Testfall: VI_02_06

4.10.1 Informationen

ID	VI_02_06
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Export des Public Key eines ECC-Schlüsselpaars (Vor-Personalisierung)
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.10.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.2.5

4.10.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_06-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_02_06-2	Key Pair-Objekt, dessen Public Key ausgegeben werden soll, ist vorhanden und wurde mittels Schlüsselgenerierung über das Kommando GENERATE ASYMMETRIC KEY PAIR mit Schlüsseldaten befüllt. (VI_02_05: Generierung eines ECC-Schlüsselpaars (Vor-Personalisierung))

4.10.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_06-3	Anwendung für: a) den Export der vorläufigen GW-Schlüssel: •.Vorläufiger TLS-Public Key GW_WAN_TLS_PUB_PRE •.Vorläufiger SIG- Public Key GW_WAN_SIG_PUB_PRE •.Vorläufiger ENC-Public Key GW_WAN_ENC_PUB_PRE b) den Export des Integrator-spezifischen Import-Schlüssels: •.Import-Public Key IMP_PUB

CN-VI_02_06-4	Die Speicherung der zugehörigen vorläufigen GW-Schlüsselpaare (siehe a)) erfolgt in den Key Pair-Objekten Key.WAN_TLS_PRE, Key.WAN_SIG_PRE bzw. Key.WAN_ENC_PRE des DF.SMGW. Die Speicherung des zugehörigen Import-Schlüsselpaares (siehe b)) erfolgt im Key Pair-Objekt Key.IMP im MF.

4.10.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.10.6 Ablauf

Schritt	Beschreibung						
1	Selektion des DF, in dem das Key Pair-Objekt liegt, dessen Public Key ausgegeben werden soll. (VI_02_01: Selektieren eines DF/EF (Vor-Personalisierung))						
2	GENERATE ASYMMETRIC KEY PAIR: Ausgabe des Public Key ohne Schlüsselgenerierung (Übergabe der Key Reference des Key Pair-Objektes, dessen Public Key ausgegeben werden soll)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	47	83	00	LL	XX...XX	XX
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist 'Le' enthält die Anzahl der zu erwartenden Oktette.						

4.10.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.11 Testfall: VI_02_07

4.11.1 Informationen

ID	VI_02_07
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Wechsel des Import-Schlüsselpaars
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.11.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.2.6

4.11.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_07-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_02_07-2	Transport-Import-Schlüsselpaar (IMP_PRV_TRANS, IMP_PUB_TRANS) (im Key Pair-Objekt Key.IMP_TRANS) sowie zusätzlich der Public Key IMP_PUB_TRANS (im Public Key-Objekt Key.IMP_PUB_TRANS) liegen im Sicherheitsmodul vor und sind aktiviert. (Hinweis: Die Anlage und Befüllung der genannten Key-Objekte ist bereits im Rahmen der Initialisierung des Sicherheitsmoduls erfolgt.)
CN-VI_02_07-3	Key Pair-Objekt Key.IMP zur Speicherung von (IMP_PRV, IMP_PUB) ist vorhanden und das Key-Attribut Key-LifeCycleStatus des Key Pair-Objektes besitzt den Wert „initialisation“ oder „operational state – deactivated“ (Hinweis: Die Anlage des Key Pair-Objektes ist bereits im Rahmen der Initialisierung des Sicherheitsmoduls erfolgt.) (VI_02_04: Deaktivieren eines Key-Objektes (Vor-Personalisierung))
CN-VI_02_07-4	Public Key-Objekt Key.IMP_PUB zur Speicherung von IMP_PUB ist vorhanden und das Key-Attribut Key-LifeCycleStatus des Public Key-Objektes besitzt den Wert „initialisation“ oder „operational state –

	deactivated“ (Hinweis: Die Anlage des Public Key-Objektes ist bereits im Rahmen der Initialisierung des Sicherheitsmoduls erfolgt.) (VI_02_04: Deaktivieren eines Key-Objektes (Vor-Personalisierung))

4.11.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_07-5	Im Rahmen der Produktion des Sicherheitsmoduls generiert der Hersteller des Sicherheitsmoduls ein Schlüsselpaar (IMP_PRV_TRANS, IMP_PUB_TRANS), mit dem der Import von Public Keys in der Phase „Vor-Personalisierung + Integration von Sicherheitsmodul und GW“ realisiert wird. Je nach Hersteller kann das Schlüsselpaar kundenspezifisch gewählt sein. Das Schlüsselpaar hat den Charakter eines Transport-Schlüsselpaares (siehe unten).
CN-VI_02_07-6	Im Auslieferungszustand enthält das initialisierte Sicherheitsmodul das Schlüsselpaar (IMP_PRV_TRANS, IMP_PUB_TRANS) im Key Pair-Objekt Key.IMP_TRANS im MF sowie zusätzlich nochmal den Public Key IMP_PUB_TRANS im Public Key-Objekt Key.IMP_PUB_TRANS im MF. Hinweis: Grund für die doppelte Speicherung des Public Key ist das Set der verfügbaren Kommandos des Sicherheitsmoduls.
CN-VI_02_07-7	Über diesen Use Case kann das Transport-Import-Schlüsselpaar (IMP_PRV_TRANS, IMP_PUB_TRANS) gegen ein Integrator-eigenes Import-Schlüsselpaar (IMP_PRV, IMP_PUB) ausgetauscht werden. Die Speicherung des neuen Import-Schlüsselpaares (IMP_PRV, IMP_PUB) erfolgt dabei im Key Pair-Objekt Key.IMP im MF, die zusätzliche Speicherung des Public Key IMP_PUB erfolgt dabei im Public Key-Objekt Key.IMP_PUB im MF.

4.11.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_07-8	Das Key-Attribut Key-LifeCycleStatus des Key Pair-Objektes Key.IMP für (IMP_PRV, IMP_PUB) besitzt nach der Schlüsselgenerierung den Wert „operational state – activated“, so dass das Key Pair-Objekt direkt zu seiner Nutzung für Krypto-Operationen bereitsteht.
CN-VI_02_07-9	Das Key-Attribut Key-LifeCycleStatus des Public Key-Objektes Key.IMP_PUB für IMP_PUB besitzt nach dem Schlüsselimport den Wert

	„operational state – activated“, so dass das Public Key-Objekt direkt zu seiner Nutzung für Krypto-Operationen bereitsteht.

4.11.6 Ablauf

Schritt	Beschreibung														
1	Durchführung von (VI_02_05: Generierung eines ECC-Schlüsselpaares (Vor-Personalisierung))														
2	GGf. Durchführung von (VI_02_06: Export des Public Key eines ECC-Schlüsselpaares (Vor-Personalisierung))														
3	Erstellung des Inputs IMP_PUB_CRTBody für das Import-Zertifikat IMP_PUB_CRT zu IMP_PUB. Für das Import-Zertifikat ist darauf zu achten, dass die dort eingetragene Key Reference mit dem Key-Attribut Key-Name des zu befüllenden Public Key-Objektes Key.IMP_PUB übereinstimmt.														
4	Durchführung von (VI_02_09: Generieren einer Signatur / DST (Vor-Personalisierung))														
5	Erstellung des Import-Zertifikates IMP_PUB_CRT zu IMP_PUB. Dies besteht aus IMP_PUB_CRTBody und Sig_IMP_PUB_CRTBody.														
6	Selektion des DF, in dem das zu befüllende Public Key-Objekt Key.IMP_PUB liegt. (VI_02_01: Selektieren eines DF/EF (Vor-Personalisierung))														
7	MSE SET (DST): Signatur- und Zertifikatverifikation (Übergabe der Key Reference des Public Key-Objektes Key.IMP_PUB_TRANS mit dem Signaturprüf Schlüssel IMP_PUB_TRANS und Übergabe des zu verwendenden Krypto-Algorithmus)														
	<table><tr><th>CLA</th><th>INS</th><th>P1</th><th>P2</th><th>Lc</th><th>Data</th><th>Le</th></tr><tr><td>00</td><td>22</td><td>81</td><td>b6</td><td>LL</td><td>XX...XX</td><td>--</td></tr></table>	CLA	INS	P1	P2	Lc	Data	Le	00	22	81	b6	LL	XX...XX	--
	CLA	INS	P1	P2	Lc	Data	Le								
	00	22	81	b6	LL	XX...XX	--								
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.														
'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus) '83-L83-Key Reference' (für das Public Key-Objekt)															
8	PSO VERIFY CERTIFICATE (Übergabe des Import-Zertifikates IMP_PUB_CRT des zu importierenden Public Key IMP_PUB; das Import-Zertifikat enthält insbesondere Key-Zusatzinformationen sowie die Key Reference des zu befüllenden Public Key-Objektes Key.IMP_PUB)														
	<table><tr><th>CLA</th><th>INS</th><th>P1</th><th>P2</th><th>Lc</th><th>Data</th><th>Le</th></tr><tr><td>00</td><td>2a</td><td>00</td><td>be</td><td>LL</td><td>XX...XX</td><td>--</td></tr></table>	CLA	INS	P1	P2	Lc	Data	Le	00	2a	00	be	LL	XX...XX	--
	CLA	INS	P1	P2	Lc	Data	Le								
00	2a	00	be	LL	XX...XX	--									

	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

4.11.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.12 Testfall: VI_02_08

4.12.1 Informationen

ID	VI_02_08
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Import eines Public Key (Vor-Personalisierung)
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.12.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.2.6

4.12.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN-VI_02_08-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_02_08-2	Import-Schlüsselpaar (IMP_PRV, IMP_PUB) (im Key Pair-Objekt Key.IMP) sowie zusätzlich der Public Key IMP_PUB (im Public Key-Objekt Key.IMP_PUB) liegen im Sicherheitsmodul vor und sind aktiviert. Hinweis: Die Anlage dieser Key-Objekte ist bereits im Rahmen der Initialisierung des Sicherheitsmoduls erfolgt. Für die Befüllung der Key-Objekte mit Schlüsseldaten siehe (VI_02_04: Deaktivieren eines Key-Objektes (Vor-Personalisierung))
CN-VI_02_08-3	Zu importierender Public Key KEY_PUB liegt vor.
CN-VI_02_08-4	Public Key-Objekt zur Speicherung von KEY_PUB ist vorhanden und das Key-Attribut Key-LifeCycleStatus des Public Key-Objektes besitzt den Wert „initialisation“ oder „operational state – deactivated“. (Hinweis: Für die Anwendung des vorliegenden Use Case ist " + "die Anlage entsprechender Public Key-Objekte bereits im " + "Rahmen der Initialisierung des Sicherheitsmoduls erfolgt.) (VI_02_04: Deaktivieren eines Key-Objektes (Vor-Personalisierung))

4.12.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_08-5	Der Import eines Public Key KEY_PUB in dieser Phase wird über ein Import-Schlüsselpaar (IMP_PRV, IMP_PUB) realisiert. Die Speicherung des Import-Schlüsselpaares (IMP_PRV, IMP_PUB) erfolgt im Key Pair-Objekt Key.IMP im MF, die zusätzliche Speicherung des Public Key IMP_PUB erfolgt im Public Key-Objekt Key.IMP_PUB im MF.

4.12.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_08-6	Das Key-Attribut Key-LifeCycleStatus des Public Key-Objektes für KEY_PUB besitzt nach dem Schlüsselimport den Wert „operational state – activated“, so dass das Public Key-Objekt direkt zu seiner Nutzung für Krypto-Operationen bereitsteht.

4.12.6 Ablauf

Schritt	Beschreibung														
1	Erstellung des Inputs KEY_PUB_CRTBody für das Import-Zertifikat KEY_PUB_CRT zu KEY_PUB. Für das Import-Zertifikat ist darauf zu achten, dass die dort eingetragene Key Reference mit dem Key-Attribut Key-Name des zu befüllenden Public Key-Objektes für KEY_PUB übereinstimmt.														
2	Zur Generierung der Signatur über KEY_PUB_CRTBody unter Nutzung des Signaturschlüssels IMP_PRV mit Ergebnis der Signatur Sig_KEY_PUB_CRTBody, Durchführung von (VI_02_09: Generieren einer Signatur / DST (Vor-Personalisierung))														
3	Erstellung des Import-Zertifikates KEY_PUB_CRT zu KEY_PUB. Dies besteht aus KEY_PUB_CRTBody und Sig_KEY_PUB_CRTBody.														
4	Selektion des DF, in dem das zu befüllende Public Key-Objekt für KEY_PUB liegt. (VI_02_01: Selektieren eines DF/EF (Vor-Personalisierung))														
5	MSE SET (DST): Signatur- und Zertifikatverifikation (Übergabe der Key Reference des Public Key-Objektes Key.IMP_PUB mit dem Signaturprüf Schlüssel IMP_PUB und Übergabe des zu verwendenden Krypto-Algorithmus)														
	<table><tr><th>CLA</th><th>INS</th><th>P1</th><th>P2</th><th>Lc</th><th>Data</th><th>Le</th></tr><tr><td>00</td><td>22</td><td>81</td><td>b6</td><td>LL</td><td>XX...XX</td><td>--</td></tr></table>	CLA	INS	P1	P2	Lc	Data	Le	00	22	81	b6	LL	XX...XX	--
	CLA	INS	P1	P2	Lc	Data	Le								
	00	22	81	b6	LL	XX...XX	--								
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.														
'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus) '83-L83-Key Reference' (für das Public Key-Objekt)															
6	PSO VERIFY CERTIFICATE (Übergabe des Import-Zertifikates KEY_PUB_CRT des zu importierenden Public Key KEY_PUB; das Import-Zertifikat enthält insbesondere Key-Zusatzinformationen sowie die Key Reference des zu befüllenden Public Key-Objektes für KEY_PUB)														
	<table><tr><th>CLA</th><th>INS</th><th>P1</th><th>P2</th><th>Lc</th><th>Data</th><th>Le</th></tr><tr><td>00</td><td>2a</td><td>00</td><td>be</td><td>LL</td><td>XX...XX</td><td>--</td></tr></table>	CLA	INS	P1	P2	Lc	Data	Le	00	2a	00	be	LL	XX...XX	--
	CLA	INS	P1	P2	Lc	Data	Le								
	00	2a	00	be	LL	XX...XX	--								
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.														
'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R S' zu verifizierende															

	Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])

4.12.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.13 Testfall: VI_02_09

4.13.1 Informationen

ID	VI_02_09
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Generieren einer Signatur / DST (Vor-Personalisierung)
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.13.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.2.7

4.13.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_09-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_02_09-2	Key Pair-Objekt mit dem Signaturschlüssel ist im Sicherheitsmodul vorhanden und ist aktiviert. (VI_02_05: Generierung eines ECC-Schlüsselpaars (Vor-Personalisierung))

4.13.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_09-3	Die Aufbereitung der zu signierenden Daten inkl. Hashen der Daten erfolgt durch das GW bzw. anderweitig außerhalb des Sicherheitsmoduls (Signaturdaten).

4.13.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.13.6 Ablauf

Schritt	Beschreibung						
1	Aufbereitung der Signaturdaten inkl. Hashing (passend zur vorgesehenen Elliptischen Kurve / Schlüssellänge des Signaturschlüssels).						
2	Bestimmung des Signaturschlüssels bzw. des zugehörigen Key Pair-Objektes (Speicherort im Filesystem, Key-ID). Selektion des DF, in dem das Key Pair-Objekt mit dem Signaturschlüssel gespeichert ist. (VI_02_01: Selektieren eines DF/EF (Vor-Personalisierung))						
3	MSE SET (DST): Signaturerzeugung (Übergabe der Key Reference des Key Pair-Objektes mit dem Signaturschlüssel und Übergabe des zu verwendenden Krypto-Algorithmus)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	22	41	b6	LL	XX...XX	--
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus) '84-01-Key Reference' (für das Key Pair-Objekt)						
4	PSO COMPUTE DIGITAL SIGNATURE (Signaturdaten))						
	CLA	INS	P1	P2	Lc	Data	Le
	00	2a	9e	9a	LL	XX...XX	XX
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.						

	'Data' enthält die zu signierende Daten als Oktett-String. 'Le' enthält die Anzahl der zu erwartenden Oktette.

4.13.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.14 Testfall: VI_02_10

4.14.1 Informationen

ID	VI_02_10
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Generieren einer Signatur / AT (Vor-Personalisierung)
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.14.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.2.7

4.14.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_10-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_02_10-2	Key Pair-Objekt mit dem Signaturschlüssel ist im Sicherheitsmodul vorhanden und ist aktiviert. (VI_02_05: Generierung eines ECC-Schlüsselpaars (Vor-Personalisierung))

4.14.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_10-3	Die Aufbereitung der zu signierenden Daten inkl. Hashen der Daten erfolgt durch das GW bzw. anderweitig außerhalb des Sicherheitsmoduls (Signaturdaten). Diese Signaturdaten bilden das zu signierende Token.
CN-VI_02_10-4	Als Signaturschlüssel wird ein Authentisierungsschlüssel (Schlüssel der Anwendungsklasse AT) verwendet.
CN-VI_02_10-5	Anwendung des Use Case im Rahmen der Erstellung eines Zertifikatsrequests zu einem vorläufigen ENC-Schlüssel. (UC_VI_03_04: Use Case „Erstellung des Zertifikatsrequest-Pakets für Gütesiegel-Zertifikate“)

4.14.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.14.6 Ablauf

Schritt	Beschreibung														
1	Aufbereitung des Tokens, d.h. der Signaturdaten inkl. Hashing (passend zur vorgesehenen Elliptischen Kurve / Schlüssellänge des Authentisierungsschlüssels).														
2	Bestimmung des Authentisierungsschlüssels bzw. des zugehörigen Key Pair-Objektes (Speicherort im Filesystem, Key-ID). Selektion des DF, in dem das Key Pair-Objekt mit dem Authentisierungsschlüssel gespeichert ist. (VI_02_01: Selektieren eines DF/EF (Vor-Personalisierung))														
3	MSE SET (AT): Interne Authentisierung (Übergabe der Key Reference des Key Pair-Objektes mit dem Authentisierungsschlüssel und Übergabe des zu verwendenden Krypto-Algorithmus)														
	<table><tr><th>CLA</th><th>INS</th><th>P1</th><th>P2</th><th>Lc</th><th>Data</th><th>Le</th></tr><tr><td>00</td><td>22</td><td>41</td><td>a4</td><td>LL</td><td>XX...XX</td><td>--</td></tr></table>	CLA	INS	P1	P2	Lc	Data	Le	00	22	41	a4	LL	XX...XX	--
	CLA	INS	P1	P2	Lc	Data	Le								
	00	22	41	a4	LL	XX...XX	--								
'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.															
'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus) '84-01-Key Reference' (für das Key Pair-Objekt)															

4	INTERNAL AUTHENTICATE (Token, d.h. Signaturdaten)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	88	00	00	LL	XX...XX	XX
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält das Token als Oktett-String. 'Le' enthält die Anzahl der zu erwartenden Oktette.						

4.14.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.15 Testfall: VI_02_11a

4.15.1 Informationen

ID	VI_02_11a
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Prüfen einer Signatur (Vor-Personalisierung)
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.15.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.2.7

4.15.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_11a-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

4.15.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_11a-2	Die Aufbereitung der zu prüfenden Daten inkl. Hashen der Daten erfolgt durch das GW bzw. anderweitig außerhalb des Sicherheitsmoduls (Signaturprüfdaten).

4.15.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.15.6 Ablauf

Schritt	Beschreibung						
1	Zusammenstellung der Signaturprüfdaten mit ihrer Signatur.						
2	Bestimmung des Signaturprüfchlüssels.						
3	PSO VERIFY DIGITAL SIGNATURE (Signaturprüfdaten, Signatur, Signaturprüfchlüssel)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	2a	00	a8	LL	XX...XX	--
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.						
	'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID 90-L90-Hash 9C-L9C-PubKey 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.						

4.15.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.16 Testfall: VI_02_11b

4.16.1 Informationen

ID	VI_02_11b
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Prüfen einer Signatur (Vor-Personalisierung)
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.16.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.2.7

4.16.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_11b-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_02_11b-2	Public Key-Objekt mit dem Signaturprüf Schlüssel ist im Sicherheitsmodul vorhanden und ist aktiviert. (VI_02_08: Import eines Public Key (Vor-Personalisierung))

4.16.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_11b-3	Die Aufbereitung der zu prüfenden Daten inkl. Hashen der Daten erfolgt durch das GW bzw. anderweitig außerhalb des Sicherheitsmoduls (Signaturprüfdaten).

4.16.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.16.6 Ablauf

Schritt	Beschreibung						
1	Zusammenstellung der Signaturprüfdaten mit ihrer Signatur.						
2	Bestimmung des Signaturprüfchlüssels bzw. des zugehörigen Public Key-Objektes (Speicherort im Filesystem, Key-Name). Selektion des DF, in dem das Public Key-Objekt mit dem Signaturprüfchlüssel gespeichert ist. (VI_02_01: Selektieren eines DF/EF (Vor-Personalisierung))						
3	MSE SET (DST): Signatur- und Zertifikatverifikation (Übergabe der Key Reference des Public Key-Objektes mit dem Signaturprüfchlüssel und Übergabe des zu verwendenden Krypto-Algorithmus)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	22	81	b6	LL	XX...XX	--
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus) '83-L83-Key Reference' (für das Public Key-Objekt)						
4	PSO VERIFY DIGITAL SIGNATURE (Signaturprüfdaten, Signatur)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	2a	00	a8	LL	XX...XX	--
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R S' (Oktett-String, R und S von gleicher Oktett-Länge)						

4.16.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.17 Testfall: VI_02_12a

4.17.1 Informationen

ID	VI_02_12a
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Auslesen eines transparenten Technischen Datenfeldes
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.17.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.2.8

4.17.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_12a-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_02_12a-2	MF ist selektiert. (VI_02_01: Selektieren eines DF/EF (Vor-Personalisierung))

4.17.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_12a-3	Anwendung auf die transparenten Technischen Datenfelder EF.SecModAccess und EF.SecModCrypto.

4.17.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.17.6 Ablauf

Schritt	Beschreibung						
1	SELECT: EF (File-ID des EF.SecModAccess bzw. EF.SecModCrypto)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	a4	02	0c	02	XX XX	--
	'Data' enthält den File-Identifizier des zu selektierenden EF.						
2	READ BINARY						
	CLA	INS	P1	P2	Lc	Data	Le
	00	b0	XX	XX	--	--	XX
	'P1' enthält $(\text{Offset} - \text{P2}) / 256$, wobei Offset aus {'0000', ..., '7FFF'}. 'P2' enthält den Offset mod 256. 'Le' enthält die Anzahl der zu erwartenden Oktette.						

4.17.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.18 Testfall: VI_02_12b

4.18.1 Informationen

ID	VI_02_12b
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Auslesen eines transparenten Technischen Datenfeldes
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.18.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.2.8

4.18.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_12b-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_02_12b-2	MF ist selektiert. (VI_02_01: Selektieren eines DF/EF (Vor-Personalisierung))

4.18.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_12b-3	Anwendung auf die transparenten Technischen Datenfelder EF.SecModAccess und EF.SecModCrypto.

4.18.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.18.6 Ablauf

Schritt	Beschreibung						
1	READ BINARY (SFI des EF.SecModAccess bzw. EF.SecModCrypto)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	b0	XX	XX	--	--	XX
	'P1' enthält '80' + SFI. 'P2' enthält den Offset aus {'00', ..., 'FF'}. 'Le' enthält die Anzahl der zu erwartenden Oktette.						

4.18.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.19 Testfall: VI_02_13a

4.19.1 Informationen

ID	VI_02_13a
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Auslesen eines Record-orientierten Technischen Datenfeldes
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.19.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.2.8

4.19.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_13a-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_02_13a-2	MF ist selektiert. (VI_02_01: Selektieren eines DF/EF (Vor-Personalisierung))

4.19.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_13a-3	Anwendung auf die Record-orientierten Technischen Datenfelder EF.SecModTRInfo und EF.SecModLifeCycle.

4.19.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.19.6 Ablauf

Schritt	Beschreibung						
1	SELECT: EF (SFI des EF.SecModAccess bzw. EF.SecModCrypto)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	a4	02	0c	02	XX XX	--
	'Data' enthält den File-Identifizier des zu selektierenden EF.						
2	READ RECORD (Record-Nummer des auszulesenden Records)						
	CLA	INS	P1	P2	Lc	Data	Le

	00	b2	XX	04	--	--	XX
	'P1' enthält die Record-Number. 'Le' enthält die Anzahl der zu erwartenden Oktette.						

4.19.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.20 Testfall: VI_02_13b

4.20.1 Informationen

ID	VI_02_13b
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Auslesen eines Record-orientierten Technischen Datenfeldes
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.20.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.2.8

4.20.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_13b-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_02_13b-2	MF ist selektiert. (VI_02_01: Selektieren eines DF/EF (Vor-

	Personalisierung))

4.20.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_13b-3	Anwendung auf die Record-orientierten Technischen Datenfelder EF.SecModTRInfo und EF.SecModLifeCycle.

4.20.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.20.6 Ablauf

Schritt	Beschreibung						
1	READ RECORD (SFI des EF.SecModTRInfo bzw. EF.SecModLifeCycle, Record-Nummer des auszulesenden Records)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	b2	XX	XX	--	--	XX
	'P1' enthält die Record-Nummer. 'P2' enthält (SFI << 3) + '04' (Read Record der Nummer wie in P1 angegeben). 'Le' enthält die Anzahl der zu erwartenden Oktette.						

4.20.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.21 Testfall: VI_02_14a

4.21.1 Informationen

ID	VI_02_14a
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Update eines Record-orientierten Technischen Datenfeldes
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.21.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.2.8

4.21.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_14a-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_02_14a-2	MF ist selektiert. (VI_02_01: Selektieren eines DF/EF (Vor-Personalisierung))
CN-VI_02_14a-3	Update-Daten für das Technische Datenfeld liegen vor.

4.21.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_14a-4	Anwendung auf das Record-orientierte Technische Datenfeld EF.SecModLifeCycle.

4.21.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.21.6 Ablauf

Schritt	Beschreibung						
1	SELECT: EF (File-ID des EF.SecModLifeCycle)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	a4	02	0c	02	XX XX	--
	'Data' enthält den File-Identifizier des zu selektierenden EF.						
2	UPDATE RECORD (Record-Nummer des zu schreibenden Records, Update-Daten)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	dc	XX	04	LL	XX...XX	--
	'P1' enthält die Record-Nummer. 'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die zu schreibenden neuen Daten.						

4.21.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.22 Testfall: VI_02_14b

4.22.1 Informationen

ID	VI_02_14b
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Update eines Record-orientierten Technischen Datenfeldes

Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.22.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.2.8

4.22.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_14b-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_02_14b-2	MF ist selektiert. (VI_02_01: Selektieren eines DF/EF (Vor-Personalisierung))
CN-VI_02_14b-3	Update-Daten für das Technische Datenfeld liegen vor.

4.22.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_02_14b-4	Anwendung auf das Record-orientierte Technische Datenfeld EF.SecModLifeCycle.

4.22.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.22.6 Ablauf

Schritt	Beschreibung
1	UPDATE RECORD (SFI des EF.SecModLifeCycle, Record-Nummer des zu schreibenden Records, Update-Daten)

	CLA	INS	P1	P2	Lc	Data	Le
	00	dc	XX	XX	LL	XX...XX	--
	'P1' enthält die Record-Number. 'P2' enthält (SFI << 3) + '04' (Update Record der Nummer wie in P1 angegeben) 'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die zu schreibenden neuen Daten.						

4.22.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.23 Testfall: VI_03_01a

4.23.1 Informationen

ID	VI_03_01a
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Import des SM-PKI-Root-Zertifikates in das Sicherheitsmodul (Vor-Personalisierung)
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.23.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.3

4.23.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_03_01a-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_03_01a-2	Zu schreibendes SM-PKI-Root-Zertifikat liegt vor.

4.23.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_03_01a-3	Die Speicherung des SM-PKI-Root-Zertifikates erfolgt im transparenten Datenfeld EF.SMPKIRoot_x (sinnvollerweise x=1 für das initiale SM-PKI-Root-Zertifikat) im DF.SMGW. Ferner erfolgt zusätzlich die Speicherung des Root-Public Key aus dem SM-PKI-Root-Zertifikat im zugehörigen Public Key-Objekt Key.SMPKIRoot_x im DF.SMGW. Die zusätzliche Speicherung des Root-Public Key erfolgt aus dem Grund, als dass das Sicherheitsmodul bei Krypto-Operationen mit dem Root-Public Key mit diesem nur in Form eines Public Key-Objektes arbeiten und hierfür nicht auf den im Zertifikat enthaltenen Public Key zurückgreifen kann.
CN-VI_03_01a-4	Hinsichtlich der Speicherung des Root-Public Key im Sicherheitsmodul hat der Integrator für die Übereinstimmung zwischen dem Root-Public Key im SM-PKI-Root-Zertifikat und dem importierten Public Key Sorge zu tragen.

4.23.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.23.6 Ablauf

Schritt	Beschreibung						
1	Selektion des DF.SMGW. (VI_02_01: Selektieren eines DF/EF (Vor-Personalisierung))						
2	SELECT: EF (File-ID des EF.SMPKIRoot_x)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	a4	02	0c	02	XX XX	--

	'Data' enthält den File-Identifizier des zu selektierenden EF.						
3	UPDATE BINARY (SM-PKI-Root-Zertifikat)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	d6	XX	XX	LL	XX...XX	--
	'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}. 'P2' enthält den Offset mod 256. 'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die zu schreibenden neuen Daten.						
4	Extrahieren des Root-Public Key aus dem SM-PKI-Root-Zertifikat.						
5	Durchführung von (VI_02_08: Import eines Public Key (Vor-Personalisierung))						
6	Nach Abschluss des Schreibens des SM-PKI-Root-Zertifikates: Angewandt auf EF.SMPKIRoot_x Durchführung von (VI_02_02: Aktivieren eines DF/EF (Vor-Personalisierung))						

4.23.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.24 Testfall: VI_03_01b

4.24.1 Informationen

ID	VI_03_01b
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Import des SM-PKI-Root-Zertifikates in das Sicherheitsmodul
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.24.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.3

4.24.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_03_01b-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_03_01b-2	Zu schreibendes SM-PKI-Root-Zertifikat liegt vor.

4.24.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_03_01b-3	Die Speicherung des SM-PKI-Root-Zertifikates erfolgt im transparenten Datenfeld EF.SMPKIRoot_x (sinnvollerweise x=1 für das initiale SM-PKI-Root-Zertifikat) im DF.SMGW. Ferner erfolgt zusätzlich die Speicherung des Root-Public Key aus dem SM-PKI-Root-Zertifikat im zugehörigen Public Key-Objekt Key.SMPKIRoot_x im DF.SMGW. Die zusätzliche Speicherung des Root-Public Key erfolgt aus dem Grund, als dass das Sicherheitsmodul bei Krypto-Operationen mit dem Root-Public Key mit diesem nur in Form eines Public Key-Objektes arbeiten und hierfür nicht auf den im Zertifikat enthaltenen Public Key zurückgreifen kann.
CN-VI_03_01b-4	Hinsichtlich der Speicherung des Root-Public Key im Sicherheitsmodul hat der Integrator für die Übereinstimmung zwischen dem Root-Public Key im SM-PKI-Root-Zertifikat und dem importierten Public Key Sorge zu tragen.

4.24.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.24.6 Ablauf

Schritt	Beschreibung						
1	Selektion des DF.SMGW. (VI_02_01: Selektieren eines DF/EF (Vor-Personalisierung))						
2	UPDATE BINARY (SFI des EF.SMPKIRoot_x, SM-PKI-Root-Zertifikat)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	d6	XX	XX	LL	XX...XX	--
	'P1' enthält '80' + SFI.						
	'P2' enthält den Offset aus {'00', ..., 'FF'}.						
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.						
	'Data' enthält die zu schreibenden neuen Daten.						
3	Extrahieren des Root-Public Key aus dem SM-PKI-Root-Zertifikat.						
4	Durchführung von (VI_02_08: Import eines Public Key (Vor-Personalisierung))						
5	Nach Abschluss des Schreibens des SM-PKI-Root-Zertifikates: Angewandt auf EF.SMPKIRoot_x Durchführung von (VI_02_02: Aktivieren eines DF/EF (Vor-Personalisierung))						

4.24.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.25 Testfall: VI_03_02

4.25.1 Informationen

ID	VI_03_02
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Generierung eines vorläufigen GW-Schlüsselpaares

Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.25.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.3

4.25.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_03_02-1	Angewandt auf die vorläufigen GW-Schlüsselpaare und deren Key Pair-Objekte: (VI_02_05: Generierung eines ECC-Schlüsselpaares (Vor-Personalisierung))

4.25.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_03_02-2	Anwendung für die onboard-Generierung der vorläufigen GW-Schlüsselpaare für die WAN-Kommunikation, d.h. • (GW_WAN_TLS_PRV_PRE, GW_WAN_TLS_PUB_PRE) • (GW_WAN_SIG_PRV_PRE, GW_WAN_SIG_PUB_PRE) • (GW_WAN_ENC_PRV_PRE, GW_WAN_ENC_PUB_PRE) Die Speicherung der vorgenannten vorläufigen GW-Schlüsselpaare erfolgt in den Key Pair-Objekten Key.WAN_TLS_PRE, Key.WAN_SIG_PRE bzw. Key.WAN_ENC_PRE im DF.SMGW.
CN-VI_03_02-3	Je nach verwendeter Kommando-Variante des Kommandos GENERATE ASYMMETRIC KEY PAIR erfolgt eine Schlüsselgenerierung mit oder ohne Ausgabe des Public Key.

4.25.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN-VI_03_02-4	Angewandt auf die vorläufigen GW-Schlüsselpaare und deren Key Pair-Objekte: (VI_02_05: Generierung eines ECC-Schlüsselpaares (Vor-Personalisierung))

4.25.6 Ablauf

Schritt	Beschreibung
1	Angewandt auf die vorläufigen GW-Schlüsselpaare und deren Key Pair-Objekte: (VI_02_05: Generierung eines ECC-Schlüsselpaares (Vor-Personalisierung))

4.25.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.26 Testfall: VI_03_03

4.26.1 Informationen

ID	VI_03_03
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Export des Public Key eines vorläufigen GW-Schlüsselpaares (Vor-Personalisierung)
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.26.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.3

4.26.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_03_03-1	Angewandt auf die vorläufigen GW-Schlüsselpaare und deren Key Pair-Objekte: (VI_02_06: Export des Public Key eines ECC-Schlüsselpaares (Vor-Personalisierung))

4.26.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_03_03-2	Anwendung für den Export der vorläufigen GW-Public Keys • GW_WAN_TLS_PUB_PRE • GW_WAN_SIG_PUB_PRE • GW_WAN_ENC_PUB_PRE sofern der Export eines Public Keys eines zuvor onboard generierten vorläufigen GW-Schlüsselpaares nicht in UC_VI_03_02: Use Case „Generierung eines vorläufigen GW-Schlüsselpaares (Vor-Personalisierung)“ erfolgt.
CN-VI_03_03-3	Die Speicherung der vorläufigen GW-Schlüsselpaare erfolgt in den Key Pair-Objekten Key.WAN_TLS_PRE, Key.WAN_SIG_PRE bzw. Key.WAN_ENC_PRE im DF.SMGW. Siehe UC_VI_03_02: Use Case „Generierung eines vorläufigen GW-Schlüsselpaares (Vor-Personalisierung)“.

4.26.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.26.6 Ablauf

Schritt	Beschreibung
1	Selektion des DF, in dem die vorläufigen GW-Schlüsselpaare und " + "deren Key Pair-Objekte liegen, dessen Public Key ausgegeben werden soll. (VI_02_01: Selektieren eines DF/EF (Vor-Personalisierung))
2	GENERATE ASYMMETRIC KEY PAIR: Ausgabe des Public Key ohne Schlüsselgenerierung (Übergabe der Key Reference des Key Pair-Objektes, dessen Public Key ausgegeben werden soll)

	CLA	INS	P1	P2	Lc	Data	Le
	00	47	83	00	LL	XX...XX	XX
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist 'Le' enthält die Anzahl der zu erwartenden Oktette.						

4.26.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.27 Testfall: VI_03_04

4.27.1 Informationen

ID	VI_03_04
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Erstellung des Zertifikatsrequest-Pakets für Gütesiegel-Zertifikate
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.27.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.3

4.27.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_03_04-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_03_04-2	Vorläufiges GW-Schlüsselpaar (GW_WAN_TLS_PRV_PRE, GW_WAN_TLS_PUB_PRE), (GW_WAN_SIG_PRV_PRE, GW_WAN_SIG_PUB_PRE) bzw. (GW_WAN_ENC_PRV_PRE, GW_WAN_ENC_PUB_PRE) wurde generiert und ist aktiviert. (VI_03_02: Generierung eines vorläufigen GW-Schlüsselpaares)

4.27.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_03_04-3	Anwendung für das Zertifikatsrequest-Paket mit den drei Zertifikatsrequests zu den vorläufigen GW-Schlüsselpaaren für die WAN-Kommunikation • (GW_WAN_TLS_PRV_PRE, GW_WAN_TLS_PUB_PRE) • (GW_WAN_SIG_PRV_PRE, GW_WAN_SIG_PUB_PRE) • (GW_WAN_ENC_PRV_PRE, GW_WAN_ENC_PUB_PRE) Für Details siehe [TR-03109-4].
CN-VI_03_04-4	Die Speicherung der vorläufigen GW-Schlüsselpaare erfolgt in den Key Pair-Objekten Key.WAN_TLS_PRE, Key.WAN_SIG_PRE bzw. Key.WAN_ENC_PRE im DF.SMGW. Siehe UC_VI_03_02: Use Case „Generierung eines vorläufigen GW-Schlüsselpaares (Vor-Personalisierung)“.
CN-VI_03_04-5	Die Generierung der Autorisierungssignatur zum Zertifikatsrequest-Paket liegt außerhalb des vorliegenden Use Case.

4.27.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.27.6 Ablauf

Schritt	Beschreibung
1	Sofern für das vorläufige Schlüsselpaar (GW_WAN_TLS_PRV_PRE, GW_WAN_TLS_PUB_PRE) in UC_VI_03_02: Use Case „Generierung eines vorläufigen GW-Schlüsselpaares (Vor-Personalisierung)“ keine Ausgabe des Public Key-Parts erfolgt ist, Durchführung von (VI_03_03: Export des Public Key eines

	vorläufigen GW-Schlüsselpaars (Vor-Personalisierung))
2	Zusammenstellung des Zertifikatsrequests zum Public Key GW_WAN_TLS_PUB_PRE. Ergebnis: ZertRequest_TLS_PRE.
3	Für die innere Signatur des Zertifikatsrequests: Aufbereitung von ZertRequest_TLS_PRE für die innere Signatur (Hashing). Ergebnis: InputSig_ZertRequest_TLS_PRE.
4	Für die innere Signatur des Zertifikatsrequests mit InputSig_ZertRequest_TLS_PRE als Signaturdaten und unter Nutzung von GW_WAN_TLS_PRV_PRE als Signaturschlüssel, Ergebnis Sig_ZertRequest_TLS_PRE: Durchführung von (VI_02_09: Generieren einer Signatur / DST (Vor-Personalisierung))
5	Zusammenstellung des finalen Zertifikatsrequests zum vorläufigen TLS- Schlüsselpaar, bestehend aus ZertRequest_TLS_PRE und Sig_ZertRequest_TLS_PRE.
6	Sofern für das vorläufige Schlüsselpaar (GW_WAN_SIG_PRV_PRE, GW_WAN_SIG_PUB_PRE) in UC_VI_03_02: Use Case „Generierung eines vorläufigen GW-Schlüsselpaars (Vor-Personalisierung)“ keine Ausgabe des Public Key-Parts erfolgt ist, Durchführung von (VI_03_03: Export des Public Key eines vorläufigen GW-Schlüsselpaars (Vor-Personalisierung))
7	Zusammenstellung des Zertifikatsrequests zum Public Key GW_WAN_SIG_PUB_PRE. Ergebnis: ZertRequest_SIG_PRE.
8	Für die innere Signatur des Zertifikatsrequests: Aufbereitung von ZertRequest_SIG_PRE für die innere Signatur (Hashing). Ergebnis: InputSig_ZertRequest_SIG_PRE.
9	Für die innere Signatur des Zertifikatsrequests mit InputSig_ZertRequest_SIG_PRE als Signaturdaten und unter Nutzung von GW_WAN_SIG_PRV_PRE als Signaturschlüssel, Ergebnis Sig_ZertRequest_SIG_PRE: Durchführung von (VI_02_09: Generieren einer Signatur / DST (Vor-Personalisierung))
10	Zusammenstellung des finalen Zertifikatsrequests zum vorläufigen SIG- Schlüsselpaar, bestehend aus ZertRequest_SIG_PRE und Sig_ZertRequest_SIG_PRE.
11	Sofern für das vorläufige Schlüsselpaar (GW_WAN_ENC_PRV_PRE, GW_WAN_ENC_PUB_PRE) in UC_VI_03_02: Use Case „Generierung eines vorläufigen GW-Schlüsselpaars (Vor-Personalisierung)“ keine Ausgabe des Public Key-Parts erfolgt ist, Durchführung von (VI_03_03: Export des Public Key eines vorläufigen GW-Schlüsselpaars (Vor-Personalisierung))
12	Zusammenstellung des Zertifikatsrequests zum Public Key GW_WAN_ENC_PUB_PRE. Ergebnis: ZertRequest_ENC_PRE.
13	Für die innere Signatur des Zertifikatsrequests: Aufbereitung von

	ZertRequest_ENC_PRE für die innere Signatur (Hashing). Ergebnis: InputSig_ZertRequest_ENC_PRE.
14	Für die innere Signatur des Zertifikatsrequests mit InputSig_ZertRequest_ENC_PRE als Signaturdaten und unter Nutzung von GW_WAN_SIG_PRV_PRE als Signaturschlüssel, Ergebnis Sig_ZertRequest_ENC_PRE: Durchführung von (VI_02_10: Generieren einer Signatur / AT (Vor-Personalisierung))
15	Zusammenstellung des finalen Zertifikatsrequests zum vorläufigen ENC-Schlüsselpaar, bestehend aus ZertRequest_ENC_PRE und Sig_ZertRequest_ENC_PRE.
16	Erstellung des Zertifikatsrequest-Pakets, bestehend aus • ZertRequest_TLS_PRE und Sig_ZertRequest_TLS_PRE • ZertRequest_SIG_PRE und Sig_ZertRequest_SIG_PRE • ZertRequest_ENC_PRE und Sig_ZertRequest_ENC_PRE Ergebnis: ZertRequestPaket_PRE.
17	Bei den vorläufigen GW-Schlüsselpaaren für die WAN-Kommunikation entfällt die äußere Signatur des Zertifikatsrequest-Pakets.

4.27.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.28 Testfall: VI_03_05a

4.28.1 Informationen

ID	VI_03_05a
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Import eines Gütesiegel-Zertifikates in das Sicherheitsmodul
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.28.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.3

4.28.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_03_05a-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_03_05a-2	Gütesiegel-Zertifikat GW_WAN_TLS_CERT_PRE, GW_WAN_SIG_CERT_PRE bzw. GW_WAN_ENC_CERT_PRE liegt im GW vor.

4.28.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_03_05a-3	Anwendung für den Import der Gütesiegel-Zertifikate • GW_WAN_TLS_CERT_PRE • GW_WAN_SIG_CERT_PRE • GW_WAN_ENC_CERT_PRE zu den vorläufigen GW-Schlüsselpaaren • (GW_WAN_TLS_PRV_PRE, GW_WAN_TLS_PUB_PRE) • (GW_WAN_SIG_PRV_PRE, GW_WAN_SIG_PUB_PRE) • (GW_WAN_ENC_PRV_PRE, GW_WAN_ENC_PUB_PRE) in das Sicherheitsmodul und dortige Speicherung.
CN-VI_03_05a-4	Die Speicherung der Gütesiegel-Zertifikate erfolgt in den transparenten Datenfeldern EF.GSCert_TLS, EF.GSCert_SIG bzw. EF.GSCert_ENC im DF.SMGW.

4.28.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.28.6 Ablauf

Schritt	Beschreibung

1	Selektion des DF.SMGW. (VI_02_01: Selektieren eines DF/EF (Vor-Personalisierung))						
2	SELECT: EF (File-ID des EF.GSCert_x mit x = TLS, SIG bzw. ENC)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	a4	02	0c	02	XX XX	--
	'Data' enthält den File-Identifizier des zu selektierenden EF.						
3	UPDATE BINARY (GW_WAN_x_CRT_PRE mit x = TLS, SIG bzw. ENC)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	d6	XX	XX	LL	XX...XX	--
	'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.						
	'P2' enthält den Offset mod 256.						
4	Nach Abschluss des Schreibens des Gütesiegel-Zertifikates angewandt auf EF.GSCert_x: Durchführung von (VI_02_02: Aktivieren eines DF/EF (Vor-Personalisierung))						
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.						
	'Data' enthält die zu schreibenden neuen Daten.						

4.28.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.29 Testfall: VI_03_05b

4.29.1 Informationen

ID	VI_03_05b
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Import eines Gütesiegel-Zertifikates in das Sicherheitsmodul
Klassifizierung	Gutfall-Test

Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.29.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.3

4.29.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_03_05b-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_03_05b-2	Gütesiegel-Zertifikat GW_WAN_TLS_CERT_PRE, GW_WAN_SIG_CERT_PRE bzw. GW_WAN_ENC_CERT_PRE liegt im GW vor.

4.29.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_03_05b-3	Anwendung für den Import der Gütesiegel-Zertifikate • GW_WAN_TLS_CERT_PRE • GW_WAN_SIG_CERT_PRE • GW_WAN_ENC_CERT_PRE zu den vorläufigen GW-Schlüsselpaaren • (GW_WAN_TLS_PRV_PRE, GW_WAN_TLS_PUB_PRE) • (GW_WAN_SIG_PRV_PRE, GW_WAN_SIG_PUB_PRE) • (GW_WAN_ENC_PRV_PRE, GW_WAN_ENC_PUB_PRE) in das Sicherheitsmodul und dortige Speicherung.
CN-VI_03_05b-4	Die Speicherung der Gütesiegel-Zertifikate erfolgt in den transparenten Datenfeldern EF.GSCert_TLS, EF.GSCert_SIG bzw. EF.GSCert_ENC im DF.SMGW.

4.29.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.29.6 Ablauf

Schritt	Beschreibung						
1	Selektion des DF.SMGW. (VI_02_01: Selektieren eines DF/EF (Vor-Personalisierung))						
2	UPDATE BINARY (SFI des EF.GSCert_x, GW_WAN_x_CRT_PRE mit x=TLS, SIG bzw. ENC)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	d6	XX	XX	LL	XX...XX	--
	'P1' enthält '80' + SFI.						
	'P2' enthält den Offset aus {'00', ..., 'FF'}.						
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.						
3	'Data' enthält die zu schreibenden neuen Daten.						
	Nach Abschluss des Schreibens des Gütesiegel-Zertifikates angewandt auf EF.GSCert_x: Durchführung von (VI_02_02: Aktivieren eines DF/EF (Vor-Personalisierung))						

4.29.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.30 Testfall: VI_04_01

4.30.1 Informationen

ID	VI_04_01
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Initiales Hochfahren des SMGW
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW

Rollen	GW

4.30.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.4

4.30.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_04_01-1	Kommando-Kommunikation zwischen GW und Sicherheitsmodul ist möglich.
CN-VI_04_01-2	PIN-Objekt zur Speicherung der GW-System-PIN ist vorhanden.

4.30.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_04_01-3	Beim Initialen Hochfahren des SMGW findet insbesondere das Pairing zwischen GW und Sicherheitsmodul statt. Die GW-System-PIN wird im Sicherheitsmodul gesetzt, genauer im PIN-Objekt PIN.GW im MF abgelegt.

4.30.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_04_01-4	Nach erfolgreicher Kommando-Ausführung ist die GW-System-PIN (als Referenzwert) im Sicherheitsmodul hinterlegt und steht nachfolgend für die Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul zur Verfügung.

4.30.6 Ablauf

Schritt	Beschreibung

1	GW-interne Generierung der GW-System-PIN. Alternativ externe Generierung der GW-System-PIN und Import in das GW.						
2	CHANGE REFERENCE DATA: Setzen der PIN (Übergabe der PIN Reference des PIN-Objektes PIN.GW sowie der GW-System-PIN selbst)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	24	01	XX	LL	XX...XX	--
	'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1. 'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die neue PIN.						

4.30.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.31 Testfall: VI_04_02a

4.31.1 Informationen

ID	VI_04_02a
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Generierung eines Keys für die Speicherverschlüsselung des GW und Import in das Sicherheitsmodul
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW

4.31.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.4

4.31.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_04_02a-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

4.31.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_04_02a-2	Die Speicherung der symmetrischen GW-Keys erfolgt im Record-orientierten Datenfeld EF.GWKeys im DF.SMGW.

4.31.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.31.6 Ablauf

Schritt	Beschreibung						
1	Generierung des GW-Keys.						
2	Selektion des DF.SMGW. (VI_02_01: Selektieren eines DF/EF (Vor-Personalisierung))						
3	SELECT: EF (File-ID des EF.GWKeys)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	a4	02	0c	02	XX XX	--
	'Data' enthält den File-Identifizier des zu selektierenden EF.						
4	UPDATE RECORD (Record-Nummer des Records für den zu schreibenden Key, GW-Key)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	dc	XX	04	LL	XX...XX	--

	'P1' enthält die Record-Number. 'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die zu schreibenden neuen Daten.
5	Nach Abschluss des Schreibens des GW-Keys, angewandt auf EF.GWKeys (sofern EF.GWKeys nicht schon aktiviert ist): Durchführung von (VI_02_02: Aktivieren eines DF/EF (Vor-Personalisierung))

4.31.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.32 Testfall: VI_04_02b

4.32.1 Informationen

ID	VI_04_02b
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Generierung eines Keys für die Speicherverschlüsselung des GW und Import in das Sicherheitsmodul
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW

4.32.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.4

4.32.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN-VI_04_02b-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

4.32.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_04_02b-2	Die Speicherung der symmetrischen GW-Keys erfolgt im Record-orientierten Datenfeld EF.GWKeys im DF.SMGW.

4.32.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.32.6 Ablauf

Schritt	Beschreibung						
1	Generierung des GW-Keys.						
2	Selektion des DF.SMGW. (VI_02_01: Selektieren eines DF/EF (Vor-Personalisierung))						
3	UPDATE RECORD (SFI des EF.GWKeys, Record-Nummer des Records für den zu schreibenden Key, GW-Key)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	dc	XX	XX	LL	XX...XX	--
	'P1' enthält die Record-Nummer.						
	'P2' enthält (SFI << 3) + '04' (Update Record der Nummer wie in P1 angegeben)						
4	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.						
	'Data' enthält die zu schreibenden neuen Daten.						
	Nach Abschluss des Schreibens des GW-Keys, angewandt auf EF.GWKeys (sofern EF.GWKeys nicht schon aktiviert ist): Durchführung von (VI_02_02: Aktivieren eines DF/EF (Vor-Personalisierung))						

4.32.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.33 Testfall: VI_05_01

4.33.1 Informationen

ID	VI_05_01
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Import der Public Keys des GW-Administrators (Vor-Personalisierung)
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.33.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.5

4.33.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_05_01-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_05_01-2	Angewandt auf den Import der Administrator-Schlüssel GWADM_TLS_PUB, GWADM_SIG_PUB, GWADM_ENC_PUB und GWADM_AUT_PUB und deren Public Key-Objekte: (VI_02_08: Import eines Public Key (Vor-Personalisierung))
CN-VI_05_01-3	„Initiale Konfigurationsdatei“ liegt vor.

4.33.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_05_01-4	Anwendung für den Import des folgenden initialen Schlüsselmaterials des GW-Administrators, das in der „Initialen Konfigurationsdatei“ geliefert wird: • GWADM_TLS_PUB • GWADM_SIG_PUB • GWADM_ENC_PUB • GWADM_AUT_PUB
CN-VI_05_01-5	Die Speicherung der vorgenannten Administrationsschlüssel des GW-Administrators erfolgt in den Public Key-Objekten Key.GWA_TLS_x, Key.GWA_SIG_x, Key.GWA_ENC_x bzw. Key.GWA_AUT_x (sinnvollerweise x=1 für das initiale Schlüsselmaterial) im MF.

4.33.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_05_01-6	Angewandt auf den Import der Administrator-Schlüssel GWADM_TLS_PUB, GWADM_SIG_PUB, GWADM_ENC_PUB und GWADM_AUT_PUB und deren Public Key-Objekte: (VI_02_08: Import eines Public Key (Vor-Personalisierung))

4.33.6 Ablauf

Schritt	Beschreibung
1	Extrahieren der Administrator-Schlüssel GWADM_TLS_PUB, GWADM_SIG_PUB, GWADM_ENC_PUB bzw. GWADM_AUT_PUB aus den in der „Initialen Konfigurationsdatei“ gelieferten Zertifikaten GWADM_TLS_CRT, GWADM_SIG_CRT, GWADM_ENC_CRT bzw. GWADM_AUT_CRT aus der SM-PKI.
2	Angewandt auf den Import der Administrator-Schlüssel GWADM_TLS_PUB, GWADM_SIG_PUB, GWADM_ENC_PUB bzw. GWADM_AUT_PUB und deren Public Key-Objekte: (VI_02_08: Import eines Public Key (Vor-Personalisierung))

4.33.7 Erwartete Ergebnisse

ID	Beschreibung

RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.34 Testfall: VI_05_02

4.34.1 Informationen

ID	VI_05_02
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Prüfung einer Zertifikatskette (Vor-Personalisierung)
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.34.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.5

4.34.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_05_02-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_05_02-2	Kette der zu prüfenden Zertifikate (bis ggf. auf das SM-PKI-Root-Zertifikat) liegt im GW vor.
CN-VI_05_02-3	Der Root-Public Key der SM-PKI liegt im Sicherheitsmodul vor und ist aktiviert. Der im Sicherheitsmodul im Public Key-Objekt Key.SMPKIRoot_x gespeicherte Root-Public Key stimmt mit dem Public Key des SM-PKI-Root-Zertifikates, das im zum Root-Public Key zugehörigen Datenfeld EF.SMPKIRoot_x im Sicherheitsmodul abgelegt ist, überein. Siehe (VI_03_01: Import des SM-PKI-Root-Zertifikates in das Sicherheitsmodul (Vor-Personalisierung))

4.34.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_05_02-4	Betrachtet wird hier die Prüfung einer Kette von X.509-Zertifikaten bis zur SM-PKI-Root im Rahmen der SM-PKI. Für Details siehe [TR-03109-4].
CN-VI_05_02-5	Die Prüfung einer Zertifikatskette baut auf der Prüfung einzelner (Zertifikats-) Signaturen auf. Für das Parsen der beteiligten X.509-Zertifikate ist das GW zuständig.
CN-VI_05_02-6	Für den Use Case wird angenommen, dass das SM-PKI-Root-Zertifikat im transparenten Datenfeld EF.SMPKIRoot_x im DF.SMGW und der Root-Public Key des Zertifikates im zugehörigen Public Key-Objekt Key.SMPKIRoot_x im DF.SMGW gespeichert ist.

4.34.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.34.6 Ablauf

Schritt	Beschreibung
1	Fortlaufende Anwendung von UC_VI_02_11: Use Case „Prüfen einer Signatur (Vor-Personalisierung)“. Für die einzelnen zu prüfenden Zertifikate ist jeweils der Zertifikatsbody und die Signatur des Zertifikates aus dem Zertifikat zu extrahieren sowie der relevante Signaturprüfchlüssel zu bestimmen und ggf. dieser Signaturprüfchlüssel in das Sicherheitsmodul zu importieren (Übergabe des Signaturprüfchlüssels im Kommando PSO VERIFY DIGITAL SIGNATURE oder Anwendung von UC_VI_02_08: Use Case „Import eines Public Key (Vor-Personalisierung)“, falls der Signaturprüfchlüssel nicht anderweitig schon im Sicherheitsmodul vorliegt.
2	Für die Prüfung gegen das SM-PKI-Root-Zertifikat: Signaturprüfchlüssel ist der im Sicherheitsmodul im Public Key-Objekt Key.SMPKIRoot_x hinterlegte Root-Public Key (der mit dem Public Key des SM-PKI-Root-Zertifikates, das im zugehörigen Datenfeld EF.SMPKIRoot_x abgelegt ist, übereinstimmt).

4.34.7 Erwartete Ergebnisse

ID	Beschreibung

RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.35 Testfall: VI_05_03

4.35.1 Informationen

ID	VI_05_03
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Prüfung der in der Initialen Konfigurationsdatei gelieferten Zertifikate des GW-Administrators (Vor-Personalisierung)
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.35.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.5

4.35.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_05_03-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_05_03-2	„Initiale Konfigurationsdatei“ liegt vor.

4.35.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

n/a

4.35.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.35.6 Ablauf

Schritt	Beschreibung
1	Aufbereitung der „Initialen Konfigurationsdatei“, insbesondere Extrahieren der Zertifikate des GW-Administrators sowie der Zertifikate in den jeweils zugehörigen Zertifikatsketten.
2	Bestimmen der Signaturprüfchlüssel für die Prüfung der einzelnen Zertifikate.
3	Für jedes der Zertifikate des GW-Administrators: Durchführung von (VI_05_02: Prüfung einer Zertifikatskette (Vor-Personalisierung))

4.35.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.36 Testfall: VI_05_04

4.36.1 Informationen

ID	VI_05_04
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Prüfung der Signatur der Initialen Konfigurationsdatei
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.36.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.5

4.36.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_05_04-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_05_04-2	„Initiale Konfigurationsdatei“ liegt vor. In dieser Datei ist insbesondere der Signaturprüf Schlüssel GWADM_SIG_PUB des GW-Administrators enthalten.

4.36.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_05_04-3	Die „Initiale Konfigurationsdatei“ ist mit dem Signaturschlüssel GWADM_SIG_PRV des GW-Administrators signiert. Diese Signatur ist unter Verwendung des zugehörigen Signaturprüfschlüssels GWADM_SIG_PUB zu prüfen.
CN-VI_05_04-4	Auch wenn der Signaturprüfschlüssel GWADM_SIG_PUB ggf. schon im Public Key-Objekt Key.GWA_SIG_x im MF gespeichert sein sollte, kann dieses Public Key-Objekt nicht zur Signaturprüfung benutzt werden, da die Zugriffsregeln des Sicherheitsmoduls für die Phase „Vor-Personalisierung + Integration von Sicherheitsmodul und GW“ eine Verwendung der Schlüssel des GW-Administrators nicht zulassen.

4.36.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.36.6 Ablauf

Schritt	Beschreibung

1	Extrahieren des Signaturprüfchlüssels GWADM_SIG_PUB des GW-Administrators aus dem zugehörigen Zertifikat in der „Initialen Konfigurationsdatei“.
2	Extrahieren der zu prüfenden Signatur der „Initialen Konfigurationsdatei“ aus derselbigen.
3	Für die Prüfung der Signatur der „Initialen Konfigurationsdatei“ unter Nutzung des Signaturprüfchlüssels GWADM_SIG_PUB (VI_02_11: Prüfen einer Signatur (Vor-Personalisierung))

4.36.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.37 Testfall: VI_05_05

4.37.1 Informationen

ID	VI_05_05
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Löschen der Import-Schlüssel (Vor-Personalisierung)
Klassifizierung	Gutfall-Test
Phase	Vor-Personalisierung + Integration von Sicherheitsmodul und GW
Rollen	GW, Integrator

4.37.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 2.5

4.37.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN-VI_05_05-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-VI_05_05-2	Angewandt auf das Löschen von allen Import-Keys und deren Key-Objekten: (VI_02_03: Löschen eines Key-Objektes (Vor-Personalisierung))

4.37.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_05_05-3	Anwendung zum Abschluss der Teilphase „Vor-Personalisierung 2“.
CN-VI_05_05-4	Mit dem Löschen aller Key-Objekte, die Import-Schlüssel für den Import von Public Keys speichern, wird die Vor-Personalisierung des Sicherheitsmoduls abgeschlossen. Ein nachfolgender Import von Public Keys und insbesondere ein nachfolgendes Update von SM-PKI-Root-Zertifikaten ist nur unter Beteiligung des GW-Administrators möglich, siehe Kap. 4.4.
CN-VI_05_05-5	Die Speicherung der Import-Schlüssel erfolgt in den Key Pair-Objekten Key.IMP_TRANS und Key.IMP sowie in den Public Key-Objekten Key.IMP_PUB_TRANS und Key.IMP_PUB im MF.

4.37.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-VI_05_05-6	Angewandt auf das Löschen von allen Import-Keys und deren Key-Objekten: (VI_02_03: Löschen eines Key-Objektes (Vor-Personalisierung))
CN-VI_05_05-7	Ein nachfolgender Import von Public Keys und insbesondere ein nachfolgendes Update von SM-PKI-Root-Zertifikaten ist nur unter Beteiligung des GW-Administrators möglich, siehe Kap. 4.4.

4.37.6 Ablauf

Schritt	Beschreibung
1	Durchführung von (VI_02_03: Löschen eines Key-Objektes (Vor-Personalisierung))

4.37.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.38 Testfall: PN_01_01

4.38.1 Informationen

ID	PN_01_01
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Auswahl und Setzen des Security Environment
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.38.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.1

4.38.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_01_01-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_01_01-2	Falls der GW-Administrator beteiligt ist: TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)

4.38.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_01_01-3	Das Auswählen und Setzen des SE wird erforderlich, sofern nicht schon bereits das für diese Phasen relevante SE gesetzt ist. Beim Start bzw. Hochfahren des Sicherheitsmoduls ist defaultmäßig das SE mit SEID = 01 gesetzt.
CN-PN_01_01-4	Ausführung ohne Secure Messaging.

4.38.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_01_01-5	Es gelten die Zugriffsregeln wie für das zur Phase „Personalisierung des SMGW“ bzw. „Normalbetrieb des SMGW“ zugeordnete Security Environment definiert. Siehe [TR-03109-2], Kap. 3.3.1, 3.3.3.3.

4.38.6 Ablauf

Schritt	Beschreibung						
1	MSE RESTORE (SEID für Phase „Personalisierung des SMGW“ bzw. „Normalbetrieb des SMGW“)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	22	f3	XX	--	--	--
	'P2' enthält den SEID.						

4.38.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.39 Testfall: PN_02_01a

4.39.1 Informationen

ID	PN_02_01a
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Auslesen eines transparenten Technischen Datenfeldes
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.39.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.2

4.39.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_02_01a-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_02_01a-2	Falls der GW-Administrator beteiligt ist: TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_02_01a-3	MF ist selektiert. (PN_04_16: Selektieren eines DF/EF)

4.39.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_02_01a-4	Anwendung auf die transparenten Technischen Datenfelder EF.SecModAccess und EF.SecModCrypto.
CN-PN_02_01a-5	Ausführung ohne Secure Messaging.

4.39.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_02_01a-6	Es gelten die Zugriffsregeln wie für das zur Phase „Personalisierung des SMGW“ bzw. „Normalbetrieb des SMGW“ zugeordnete Security Environment definiert. Siehe [TR-03109-2], Kap. 3.3.1, 3.3.3.3.

4.39.6 Ablauf

Schritt	Beschreibung						
1	SELECT: EF (File-ID des EF.SecModAccess bzw. EF.SecModCrypto)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	a4	01	0c	02	XX XX	--
	'Data' enthält den File-Identifizier des zu selektierenden DF.						
2	READ BINARY						
	CLA	INS	P1	P2	Lc	Data	Le
	00	b0	XX	XX	--	--	XX
	'P1' enthält $(\text{Offset} - \text{P2}) / 256$, wobei Offset aus {'0000', ..., '7FFF'}. 'P2' enthält den Offset mod 256. 'Le' enthält die Anzahl der zu erwartenden Oktette.						

4.39.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.40 Testfall: PN_02_01b

4.40.1 Informationen

ID	PN_02_01b
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Auslesen eines transparenten Technischen Datenfeldes
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.40.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.2

4.40.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_02_01b-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_02_01b-2	Falls der GW-Administrator beteiligt ist: TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_02_01b-3	MF ist selektiert. (PN_04_16: Selektieren eines DF/EF)

4.40.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_02_01b-4	Anwendung auf die transparenten Technischen Datenfelder EF.SecModAccess und EF.SecModCrypto.
CN-PN_02_01b-5	Ausführung ohne Secure Messaging.

4.40.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.40.6 Ablauf

Schritt	Beschreibung						
1	READ BINARY (SFI des EF.SecModAccess bzw. EF.SecModCrypto)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	b0	XX	XX	--	--	XX
	'P1' enthält '80' + SFI. 'P2' enthält den Offset aus {'00', ..., 'FF'}. 'Le' enthält die Anzahl der zu erwartenden Oktette.						

4.40.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.41 Testfall: PN_02_02a

4.41.1 Informationen

ID	PN_02_02a
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Auslesen eines Record-orientierten Technischen Datenfeldes
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.41.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.2

4.41.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_02_02a-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_02_02a-2	Für das Technische Datenfeld EF.SecModLifeCycle: Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_02_02a-3	Falls der GW-Administrator beteiligt ist: TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_02_02a-4	MF ist selektiert. (PN_04_16: Selektieren eines DF/EF)

4.41.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_02_02a-5	Anwendung auf die Record-orientierten Technischen Datenfelder EF.SecModTRInfo und EF.SecModLifeCycle.
CN-PN_02_02a-6	Für das Technische Datenfeld EF.SecModTRInfo erfolgt die Ausführung der Kommandos ohne Secure Messaging, für das Technische Datenfeld EF.SecModLifeCycle mit Secure Messaging.

4.41.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.41.6 Ablauf

Schritt	Beschreibung

1	SELECT: EF (File-ID des EF.SecModTRInfo bzw. EF.SecModLifeCycle)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	a4	02	0c	02	XX XX	--
	'Data' enthält den File-Identifizier des zu selektierenden EF.						
2	READ RECORD (Record-Nummer des auszulesenden Records)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	b2	XX	04	--	--	XX
	'P1' enthält die Record-Nummer. 'Le' enthält die Anzahl der zu erwartenden Oktette.						

4.41.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.42 Testfall: PN_02_02b

4.42.1 Informationen

ID	PN_02_02b
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Auslesen eines Record-orientierten Technischen Datenfeldes
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.42.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.2

4.42.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_02_02b-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_02_02b-2	Für das Technische Datenfeld EF.SecModLifeCycle: Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_02_02b-3	Falls der GW-Administrator beteiligt ist: TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_02_02b-4	MF ist selektiert. (PN_04_16: Selektieren eines DF/EF)

4.42.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_02_02b-5	Anwendung auf die Record-orientierten Technischen Datenfelder EF.SecModTRInfo und EF.SecModLifeCycle.
CN-PN_02_02b-6	Für das Technische Datenfeld EF.SecModTRInfo erfolgt die Ausführung der Kommandos ohne Secure Messaging, für das Technische Datenfeld EF.SecModLifeCycle mit Secure Messaging.

4.42.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.42.6 Ablauf

Schritt	Beschreibung

1	READ RECORD (SFI des EF.SecModTRInfo bzw. EF.SecModLifeCycle, Record-Nummer des auszulesenden Records)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	b2	XX	XX	--	--	XX
	'P1' enthält die Record-Nummer. 'P2' enthält (SFI << 3) + '04' (Read Record der Nummer wie in P1 angegeben). 'Le' enthält die Anzahl der zu erwartenden Oktette.						

4.42.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.43 Testfall: PN_02_03a

4.43.1 Informationen

ID	PN_02_03a
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Update eines Record-orientierten Technischen Datenfeldes
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.43.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.2

4.43.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_02_03a-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_02_03a-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_02_03a-3	Falls der GW-Administrator beteiligt ist: TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_02_03a-4	MF ist selektiert. (PN_04_16: Selektieren eines DF/EF)
CN-PN_02_03a-5	Update-Daten für das Technische Datenfeld liegen vor.

4.43.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_02_03a-6	Anwendung auf das Record-orientierte Technische Datenfeld EF.SecModLifeCycle.
CN-PN_02_03a-7	Ausführung mit Secure Messaging

4.43.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.43.6 Ablauf

Schritt	Beschreibung						
1	SELECT: EF (File-ID des EF.SecModLifeCycle)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	a4	02	0c	02	XX XX	--

	'Data' enthält den File-Identifizier des zu selektierenden EF.						
2	UPDATE RECORD (Record-Nummer des zu schreibenden Records, Update-Daten)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	dc	XX	04	LL	XX...XX	--
	'P1' enthält die Record-Nummer. 'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die zu schreibenden neuen Daten.						

4.43.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.44 Testfall: PN_02_03b

4.44.1 Informationen

ID	PN_02_03b
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Update eines Record-orientierten Technischen Datenfeldes
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.44.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.2

4.44.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_02_03b-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_02_03b-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_02_03b-3	Falls der GW-Administrator beteiligt ist: TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_02_03b-4	MF ist selektiert. (PN_04_16: Selektieren eines DF/EF)
CN-PN_02_03b-5	Update-Daten für das Technische Datenfeld liegen vor.

4.44.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_02_03b-6	Anwendung auf das Record-orientierte Technische Datenfeld EF.SecModLifeCycle.
CN-PN_02_03b-7	Ausführung mit Secure Messaging

4.44.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.44.6 Ablauf

Schritt	Beschreibung						
1	UPDATE RECORD (SFI des EF.SecModLifeCycle, Record-Nummer des zu schreibenden Records, Update-Daten)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	dc	XX	XX	LL	XX...XX	--

	'P1' enthält die Record-Number. 'P2' enthält (SFI << 3) + '04' (Update Record der Nummer wie in P1 angegeben) 'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die zu schreibenden neuen Daten.

4.44.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.45 Testfall: PN_03_01

4.45.1 Informationen

ID	PN_03_01
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: PACE-Authentisierung
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW

4.45.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.3

4.45.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_03_01-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

CN-PN_03_01-2	MF ist selektiert. (PN_04_16: Selektieren eines DF/EF)
CN-PN_03_01-3	GW-System-PIN ist im Sicherheitsmodul im PIN-Objekt PIN.GW als Referenzwert vorhanden.

4.45.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_03_01-4	Die Speicherung der GW-System-PIN erfolgt im PIN-Objekt PIN.GW im MF.
CN-PN_03_01-5	Ausführung ohne Secure Messaging.

4.45.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_03_01-6	Die erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul setzt im Sicherheitsmodul den Sicherheitszustand PACE. Ferner besteht ein sicherer Kanal zwischen GW und Sicherheitsmodul für den nachfolgenden Datenverkehr.

4.45.6 Ablauf

Schritt	Beschreibung						
1	MSE SET (AT): PACE (Übergabe der PIN Reference des PIN-Objektes PIN.GW)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	22	c1	a4	LL	XX...XX	--
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.						
	'Data' enthält die Daten: '80-L80-OID PACE-Protokoll' (nur Wert ohne Tag '06') '83-01-PIN Reference' für das PIN-Objekt '84-L84-ID der Ellipt. Kurve' (notwendig, da mehrere Ellipt. Kurven für das PACE-Protokoll möglich sind; ID gemäß [TR-03110-3])						
2	GENERAL AUTHENTICATE: PACE (Kommando-Sequenz aus mehreren Kommandos)						

	CLA	INS	P1	P2	Lc	Data	Le
	XX	86	00	00	LL	XX...XX	XX
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: PACE-Protokoll 1. Protokollschritt: --- 2. Protokollschritt: '81-L81-Mapping Data' 3. Protokollschritt: '83-L83-Ephemeral Public Key' (hier: Public Key des GW) 4. Protokollschritt: '85-L85-Authentication Token' (hier: Token des GW) 'Le' enthält die Anzahl der zu erwartenden Oktette.						

4.45.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.46 Testfall: PN_03_02

4.46.1 Informationen

ID	PN_03_02
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Wechsel der GW-System-PIN
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.46.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.3

4.46.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_03_02-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_03_02-2	MF ist selektiert. (PN_04_16: Selektieren eines DF/EF)
CN-PN_03_02-3	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. Das PACE-Protokoll wird unter Verwendung der alten GW-System-PIN, die im GW vorliegt sowie im Sicherheitsmodul im PIN-Objekt PIN.GW als Referenzwert hinterlegt ist, durchgeführt. (PN_03_01: PACE-Authentisierung)
CN-PN_03_02-4	Falls der GW-Administrator beteiligt ist: TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_03_02-5	Neue GW-System-PIN liegt im GW vor.

4.46.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_03_02-6	Betrachtet wird der Wechsel der GW-System-PIN, die im Rahmen des PACE-Protokolls zwischen GW und Sicherheitsmodul Verwendung findet und im Sicherheitsmodul im PIN-Objekt PIN.GW abgelegt ist.
CN-PN_03_02-7	Ausführung mit Secure Messaging.

4.46.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_03_02-8	Ein Wechsel der GW-System-PIN über das Kommando CHANGE REFERENCE DATA bedingt nicht notwendig ein Zurücksetzen des Sicherheitszustandes PACE oder ein Schließen des bestehenden sicheren Kanals zwischen GW und Sicherheitsmodul, der zuvor über das PACE-Protokoll mit der alten GW-System-PIN aufgebaut wurde. Es wird daher empfohlen, über den Aufruf des Kommandos MANAGE CHANNEL

	explizit ein Zurücksetzen des Sicherheitszustandes PACE (inklusive Schließen des sicheren Kanals und Löschen der zugehörigen Session Keys) herbeizuführen (UC_PN_03_03: Use Case „Zurücksetzen des Sicherheitszustandes PACE“). Für nachfolgende Zugriffe auf das Sicherheitsmodul, die einen gesetzten Sicherheitszustand PACE bzw. einen sicheren Kanal zwischen GW und Sicherheitsmodul erfordern, ist bei Umsetzung der Empfehlung dann das PACE-Protokoll erneut - nun mit der neuen GW-System-PIN - erfolgreich auszuführen (UC_PN_03_01: Use Case „PACE-Authentisierung“).

4.46.6 Ablauf

Schritt	Beschreibung						
1	CHANGE REFERENCE DATA: Wechseln der PIN (Übergabe der PIN Reference des PIN-Objektes PIN.GW sowie von alter und neuer GW-System-PIN)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	24	00	XX	LL	XX...XX	--
	'P2' enthält die PIN-Reference nach ISO 7816-4, Kap. 11.5.1. 'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält 'Alte PIN' 'Neue PIN'.						

4.46.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.47 Testfall: PN_03_03

4.47.1 Informationen

ID	PN_03_03
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Zurücksetzen des Sicherheitszustandes PACE

Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.47.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.3

4.47.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_03_03-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_03_03-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_03_03-3	Falls der GW-Administrator beteiligt ist: TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)

4.47.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_03_03-4	Anwendung zum gezielten Zurücksetzen eines gesetzten Sicherheitszustandes PACE im Sicherheitsmodul in Verbindung mit dem Schließen des bestehenden sicheren Kanals zwischen GW und Sicherheitsmodul, der zuvor über das PACE-Protokoll mit der GW-System-PIN aufgebaut wurde, sowie in Verbindung mit dem Löschen zugehöriger Session Keys.
CN-PN_03_03-5	Ausführung ohne Secure Messaging.

4.47.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_03_03-6	Siehe Nachbedingungen in UC_PN_04_23: Use Case „Zurücksetzen der Applikationsebene des Sicherheitsmoduls“. Die erfolgreiche Ausführung des Kommandos MANAGE CHANNEL führt insbesondere zum Zurücksetzen des Sicherheitszustandes PACE, der die gegenseitige Authentisierung und den sicheren Kanal zwischen GW und Sicherheitsmodul anzeigt. Für nachfolgende Zugriffe auf das Sicherheitsmodul, die einen gesetzten Sicherheitszustand PACE bzw. einen sicheren Kanal zwischen GW und Sicherheitsmodul erfordern, ist das PACE-Protokoll erneut erfolgreich auszuführen. (PN_03_01: PACE-Authentisierung)

4.47.6 Ablauf

Schritt	Beschreibung
1	Durchführung von (PN_04_23: Terminieren des Sicherheitsmoduls)

4.47.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.48 Testfall: PN_03_04a

4.48.1 Informationen

ID	PN_03_04a
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Auslesen eines symmetrischen GW-Keys
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-

	Usage) des SMGW
Rollen	GW

4.48.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.3

4.48.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_03_04a-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_03_04a-2	MF ist selektiert. (PN_04_16: Selektieren eines DF/EF)
CN-PN_03_04a-3	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_03_04a-4	DF.SMGW ist selektiert. (PN_04_16: Selektieren eines DF/EF)

4.48.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_03_04a-5	Die Speicherung der symmetrischen GW-Keys erfolgt im Record-orientierten Datenfeld EF.GWKeys im DF.SMGW.
CN-PN_03_04a-6	Ausführung mit Secure Messaging.

4.48.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.48.6 Ablauf

Schritt	Beschreibung

1	SELECT: EF (File-ID des EF.GWKeys)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	a4	02	0c	02	XX XX	--
	'Data' enthält den File-Identifizier des zu selektierenden EF.						
2	READ RECORD (Record-Nummer des Records mit dem auszulesenden Key)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	b2	XX	04	--	--	XX
	'P1' enthält die Record-Nummer. 'Le' enthält die Anzahl der zu erwartenden Oktette.						

4.48.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.49 Testfall: PN_03_04b

4.49.1 Informationen

ID	PN_03_04b
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Auslesen eines symmetrischen GW-Keys
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW

4.49.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.3

4.49.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_03_04b-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_03_04b-2	MF ist selektiert. (PN_04_16: Selektieren eines DF/EF)
CN-PN_03_04b-3	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_03_04b-4	DF.SMGW ist selektiert. (PN_04_16: Selektieren eines DF/EF)

4.49.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_03_04b-5	Die Speicherung der symmetrischen GW-Keys erfolgt im Record-orientierten Datenfeld EF.GWKeys im DF.SMGW.
CN-PN_03_04b-6	Ausführung mit Secure Messaging.

4.49.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.49.6 Ablauf

Schritt	Beschreibung						
1	READ RECORD (SFI des EF.GWKeys, Record-Nummer des Records mit dem auszulesenden Key)						
	CLA	INS	P1	P2	Lc	Data	Le

	00	b2	XX	XX	--	--	XX
	'P1' enthält die Record-Number. 'P2' enthält (SFI << 3) + '04' (Read Record der Nummer wie in P1 angegeben). 'Le' enthält die Anzahl der zu erwartenden Oktette.						

4.49.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.50 Testfall: PN_03_05a

4.50.1 Informationen

ID	PN_03_05a
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Update eines symmetrischen GW-Keys
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW

4.50.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.3

4.50.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_03_05a-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

CN-PN_03_05a-2	MF ist selektiert. (PN_04_16: Selektieren eines DF/EF)
CN-PN_03_05a-3	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_03_05a-4	DF.SMGW ist selektiert. (PN_04_16: Selektieren eines DF/EF)
CN-PN_03_05a-5	Zu schreibender GW-Key liegt vor.

4.50.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_03_05a-6	Die Speicherung der symmetrischen GW-Keys erfolgt im Record-orientierten Datenfeld EF.GWKeys im DF.SMGW.
CN-PN_03_05a-7	Ausführung mit Secure Messaging.

4.50.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.50.6 Ablauf

Schritt	Beschreibung						
1	SELECT: EF (File-ID des EF.GWKeys)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	a4	02	0c	02	XX XX	--
	'Data' enthält den File-Identifizier des zu selektierenden EF.						
2	UPDATE RECORD (Record-Nummer des Records für den zu schreibenden Key, GW-Key)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	dc	XX	04	LL	XX...XX	--
	'P1' enthält die Record-Nummer.						

	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die zu schreibenden neuen Daten.

4.50.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.51 Testfall: PN_03_05b

4.51.1 Informationen

ID	PN_03_05b
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Update eines symmetrischen GW-Keys
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW

4.51.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.3

4.51.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_03_05b-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_03_05b-2	MF ist selektiert. (PN_04_16: Selektieren eines DF/EF)

CN-PN_03_05b-3	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_03_05b-4	DF.SMGW ist selektiert. (PN_04_16: Selektieren eines DF/EF)
CN-PN_03_05b-5	Zu schreibender GW-Key liegt vor.

4.51.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_03_05b-6	Die Speicherung der symmetrischen GW-Keys erfolgt im Record-orientierten Datenfeld EF.GWKeys im DF.SMGW.
CN-PN_03_05b-7	Ausführung mit Secure Messaging.

4.51.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.51.6 Ablauf

Schritt	Beschreibung						
1	SELECT: EF (File-ID des EF.GWKeys)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	a4	02	0c	02	XX XX	--
	'Data' enthält den File-Identifizier des zu selektierenden EF.						
2	UPDATE RECORD (SFI des EF.GWKeys, Record-Nummer des Records für den zu schreibenden Key, GW-Key)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	dc	XX	XX	LL	XX...XX	--
	'P1' enthält die Record-Nummer. 'P2' enthält (SFI << 3) + '04' (Update Record der Nummer wie in P1 angegeben)						

	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die zu schreibenden neuen Daten.

4.51.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.52 Testfall: PN_04_01

4.52.1 Informationen

ID	PN_04_01
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.52.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.1

4.52.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_01-1	Unter Verwendung des hier vorliegenden Schlüsselmaterials: (PN_05_05: Aufbau eines TLS-Kanals zwischen externer Welt und SMGW / SMGW in der Rolle TLS-Client)

4.52.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_01-2	Siehe die Ausführungen zum allgemeinen Anwendungsfall UC_PN_05_05: Use Case „Aufbau eines TLS-Kanals zwischen externer Welt und SMGW / SMGW in der Rolle TLS-Client“.
CN-PN_04_01-3	Relevante Keys in der Phase Personalisierung: • Vorläufiges TLS-Key Pair (GW_WAN_TLS_PRV_PRE, GW_WAN_TLS_PUB_PRE) des GW im Sicherheitsmodul • TLS-Key Pair (GWADM_TLS_PRV, GWADM_TLS_PUB) des GW-Administrators
CN-PN_04_01-4	Relevante Keys in der Phase Normalbetrieb: • Betriebs-TLS-Key Pair (GW_WAN_TLS_PRV, GW_WAN_TLS_PUB) des GW im Sicherheitsmodul • TLS-Key Pair (GWADM_TLS_PRV, GWADM_TLS_PUB) des GW-Administrators
CN-PN_04_01-5	Ausführung mit Secure Messaging.

4.52.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_01-6	Unter Verwendung des hier vorliegenden Schlüsselmaterials: (PN_05_05: Aufbau eines TLS-Kanals zwischen externer Welt und SMGW / SMGW in der Rolle TLS-Client)

4.52.6 Ablauf

Schritt	Beschreibung
1	Unter Verwendung des hier vorliegenden Schlüsselmaterials: (PN_05_05: Aufbau eines TLS-Kanals zwischen externer Welt und SMGW / SMGW in der Rolle TLS-Client)

4.52.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des

	Testfalls.

4.53 Testfall: PN_04_02

4.53.1 Informationen

ID	PN_04_02
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.53.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.1

4.53.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_02-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_04_02-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_04_02-3	TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_04_02-4	AUT-Key Pair (GWADM_AUT_PRV, GWADM_AUT_PUB) des GW-Administrators existiert.
CN-PN_04_02-5	Public Key GWADM_AUT_PUB des GW-Administrators liegt im Sicherheitsmodul vor und ist aktiviert. (Aus der Phase „Vor-Personalisierung + Integration von Sicherheitsmodul und GW“ ist das

	Schlüsselmaterial bereits im Sicherheitsmodul vorhanden, bzw. für Schlüsselwechsel siehe UC_PN_04_11: Use Case „Import eines Public Key“, ggf. UC_PN_04_07: Use Case „Aktivieren eines Key-Objektes“.) Der Public Key GWADM_AUT_PUB ist im Public Key-Objekt Key.GWA_AUT_x (x=1 oder 2) im MF gespeichert.

4.53.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_02-6	Relevantes Schlüsselmaterial: • AUT-Key Pair (GWADM_AUT_PRV, GWADM_AUT_PUB) des GW-Administrators
CN-PN_04_02-7	Das Public Key-Objekt für den Public Key GWADM_AUT_PUB ist durch Key.GWA_AUT_x (x=1 oder 2) im MF gegeben.
CN-PN_04_02-8	Ausführung mit Secure Messaging.

4.53.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_02-9	Erfolgreiche Ausführung der Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul setzt im Sicherheitsmodul den Sicherheitszustand AUTH.

4.53.6 Ablauf

Schritt	Beschreibung						
1	MSE SET (AT): Externe Authentisierung (Übergabe der Key Reference des Public Key-Objektes für GWADM_AUT_PUB als Authentisierungsschlüssel und Übergabe des zu verwendenden Krypto-Algorithmus)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	22	81	a4	LL	XX...XX	--
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.						
	'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus) '83-L83-Key Reference' (für das Public Key-Objekt)						

2	GET CHALLENGE ((16 Byte Challenge wie für das folgende Kommando EXTERNAL AUTHENTICATE benötigt)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	84	XX	00	--	--	XX
	'P1' enthält '00': generierte Zufallszahl wird intern gespeichert '01': generierte Zufallszahl wird intern nicht gespeichert. 'Le' enthält die Anzahl der Oktette zu erwartenden Zufallszahl (Hersteller-abhängig und in Abhängigkeit vom Ausgabeformat).						
3	Übermittlung der Challenge an den GW-Administrator (im bestehenden TLS-Kanal zwischen GW-Administrator und GW).						
4	Generierung des Authentisierungstokens durch den GW-Administrator unter Verwendung von GWADM_AUT_PRV.						
5	Übermittlung des Authentisierungstokens vom GW-Administrator an das GW (im bestehenden TLS-Kanal zwischen GW-Administrator und GW).						
6	EXTERNAL AUTHENTICATE (Authentisierungstoken des GW-Administrators)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	82	00	00	LL	XX...XX	XX
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält den Authentisierungstoken als Oktett-String.						

4.53.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.54 Testfall: PN_04_03

4.54.1 Informationen

ID	PN_04_03

Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Zurücksetzen des Sicherheitszustandes AUTH
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.54.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.1

4.54.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_03-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_04_03-2	TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_04_03-3	Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (PN_04_02: Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul)

4.54.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_03-4	Anwendung zum gezielten Zurücksetzen eines gesetzten Sicherheitszustandes AUTH im Sicherheitsmodul zum Abschluss der Administrationstätigkeiten des GW-Administrators.
CN-PN_04_03-5	Ausführung ohne Secure Messaging.

4.54.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_03-6	Siehe Nachbedingungen in UC_PN_04_23: Use Case „Zurücksetzen der Applikationsebene des Sicherheitsmoduls“. Die erfolgreiche Ausführung des Kommandos MANAGE CHANNEL führt insbesondere zum Zurücksetzen des Sicherheitszustandes AUTH, der die Administrationstätigkeiten am Sicherheitsmodul absichert. Nachfolgende Administrationstätigkeiten des GW-Administrators erfordern eine erneute Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul (UC_PN_04_02: Use Case „Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul“).

4.54.6 Ablauf

Schritt	Beschreibung
1	Durchführung von (PN_04_23: Terminieren des Sicherheitsmoduls)

4.54.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.55 Testfall: PN_04_04

4.55.1 Informationen

ID	PN_04_04
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Wechsel des GW-Administrators
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW

Rollen	GW, GW_Administrator

4.55.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.1

4.55.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_04-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_04_04-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_04_04-3	TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_04_04-4	Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (PN_04_02: Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul)
CN-PN_04_04-5	Public Key-Objekt Key.GWA_SIG_1 ist vorhanden, ist mit Schlüsseldaten gefüllt und ist aktiviert. GGf. (PN_04_07: Aktivieren eines Key-Objektes)

4.55.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_04-6	Der Wechsel des GW-Administrators ist mit dem Wechsel der Administrationsschlüssel des GW-Administrators verbunden.
CN-PN_04_04-7	Über das Initialisierungsfile des Sicherheitsmoduls sind bereits zwei Sätze von Public Key-Objekten für die Administrationsschlüssel des GW-Administrators angelegt (x=1 bzw. 2): • Public Key-Objekt Key.GWA_TLS_x für die Ablage des TLS-Public Key des GW-Administrators • Public Key-Objekt Key.GWA_SIG_x für die Ablage des SIG-Public Key des GW-Administrators • Public Key-Objekt Key.GWA_ENC_x für die Ablage des ENC-Public Key des GW-

	Administrators • Public Key-Objekt Key.GWA_AUT_x für die Ablage des AUT-Public Key des GW-Administrators
CN-PN_04_04-8	Der Use Case betrachtet den Fall, dass die Administrationsschlüssel des alten GW-Administrators in den o.g. Public Key-Objekten für x=1 abgelegt sind und die Administrationsschlüssel des neuen GW-Administrators in den o.g. Public Key-Objekten für x=2 abgelegt werden sollen, um ein direktes Überschreiben der alten Administrationsschlüssel zu vermeiden.
CN-PN_04_04-9	Der Import der neuen Administrationsschlüssel erfordert die Mitwirkung des alten GW-Administrators.
CN-PN_04_04-10	Ausführung mit Secure Messaging.

4.55.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_04-11	Sofern durch den alten GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (PN_04_03: Zurücksetzen des Sicherheitszustandes AUTH)
CN-PN_04_04-12	Sobald die Administrationsschlüssel des alten GW-Administrators nicht mehr benötigt werden und nur noch der neue GW-Administrator Administrationstätigkeiten am Sicherheitsmodul vornehmen (können) soll, wird empfohlen, die entsprechenden Public Key-Objekte, hier also Key.GWA_TLS_1, Key.GWA_SIG_1, Key.GWA_ENC_1 und Key.GWA_AUT_1 zu deaktivieren (UC_PN_04_08: Use Case „Deaktivieren eines Key-Objektes“). Bei einer Deaktivierung der Public Keys des alten GW-Administrators sollte aber dafür Sorge getragen werden, dass zuvor die Public Keys des neuen GW-Administrators (hier: Public Key-Objekte Key.GWA_TLS_2, Key.GWA_SIG_2, Key.GWA_ENC_2 und Key.GWA_AUT_2) aktiviert wurden (UC_PN_04_07: Use Case „Aktivieren eines Key-Objektes“), damit der neue GW-Administrator die weiteren Administrationstätigkeiten vornehmen kann.

4.55.6 Ablauf

Schritt	Beschreibung
1	Wiederholte Durchführung von UC_PN_04_13: Use Case „Prüfung einer

	Zertifikatskette (SM-PKI)“ für die Prüfung der Zertifikate zu den Public Keys des neuen GW-Administrators.
2	Wiederholte Durchführung von UC_PN_04_11: Use Case „Import eines Public Key“ für den Import der Public Keys des neuen GW-Administrators. Die für den Import der Public Keys erforderlichen Import-Zertifikate werden dabei durch den alten GW-Administrator erstellt und mit seinem privaten Signaturschlüssel (passend zum in Key.GWA_SIG_1 gespeicherten Public Key) signiert. Ferner werden in den Import-Zertifikaten die mit den Public Keys des neuen GW-Administrators zu befüllenden Public Key-Objekte entsprechend referenziert, derart dass der neue TLS-Public Key im Public Key-Objekt Key.GWA_TLS_2, der neue SIG-Public Key im Public Key-Objekt Key.GWA_SIG_2, der neue ENC-Public Key im Public Key-Objekt Key.GWA_ENC_2 und der neue AUT-Public Key im Public Key-Objekt Key.GWA_AUT_2 gespeichert werden.
3	Sollen die Public Keys des neuen GW-Administrators zunächst noch nicht aktiv sein, so Anwendung von UC_PN_04_08: Use Case „Deaktivieren eines Key-Objektes“ zur Deaktivierung der entsprechenden Public Key-Objekte, hier also Key.GWA_TLS_2, Key.GWA_SIG_2, 48 Bundesamt für Sicherheit in der Informationstechnik Personalisierung, Normalbetrieb (End-Usage) und Außerbetriebnahme des SMGW 4 Key.GWA_ENC_2 und Key.GWA_AUT_2.
4	Sollen anschließend zu gegebener Zeit die Public Keys des neuen GW-Administrators aktiv geschaltet werden, so Anwendung von UC_PN_04_07: Use Case „Aktivieren eines Key-Objektes“ zur Aktivierung der entsprechenden Public Key-Objekte, hier also Key.GWA_TLS_2, Key.GWA_SIG_2, Key.GWA_ENC_2 und Key.GWA_AUT_2.

4.55.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.56 Testfall: PN_04_05

4.56.1 Informationen

ID	PN_04_05
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Anlegen eines Key-Objektes

Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.56.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.2

4.56.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_05-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_04_05-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_04_05-3	TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_04_05-4	Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (PN_04_02: Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul)

4.56.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_05-5	Ausführung mit Secure Messaging.

4.56.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN-PN_04_05-6	Bei der Anlage eines Key-Objektes über das Kommando CREATE KEY besitzt das Key-Attribut Key-LifeCycleStatus den Wert „initialisation“. Vor Nutzung des Key-Objektes z.B. für Krypto-Operationen ist dieses mit Schlüsseldaten zu füllen. Für ein Key Pair-Objekt erfolgt dies mittels des Kommandos GENERATE ASYMMETRIC KEY PAIR, siehe UC_PN_04_09: Use Case „Generierung eines ECC-Schlüsselpaares“; für ein Public Key-Objekt erfolgt dies mittels des Kommandos PSO VERIFY CERTIFICATE, siehe UC_PN_04_11: Use Case „Import eines Public Key“).
CN-PN_04_05-7	Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (PN_04_03: Zurücksetzen des Sicherheitszustandes AUTH)

4.56.6 Ablauf

Schritt	Beschreibung						
1	Selektion des DF, in dem das neue Key-Objekt angelegt werden soll. (PN_04_16: Selektieren eines DF/EF)						
2	CREATE KEY (Übergabe der Key Reference des anzulegenden Key-Objektes inkl. weiterer Informationen zum Key-Objekt)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	e0	81	00	LL	XX...XX	--
'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Key-Daten inkl. der Key-Reference: '62-L62- AD-LAD- 83-L83-KID/KeyName 96-L96-KeyUsageCounterInit A1-00 bzw. A2-00 7B-L7B- A4-LA4-(80-L80-CryptoID) (A4-LA4-(80-L80-CryptoID)) bzw. B6-LB6-(80-L80-CryptoID) (B6-LB6-(80-L80-CryptoID))'							

4.56.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.57 Testfall: PN_04_06

4.57.1 Informationen

ID	PN_04_06
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Löschen eines Key-Objektes
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.57.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.2

4.57.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_06-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_04_06-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_04_06-3	TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_04_06-4	Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (PN_04_02: Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul)
CN-PN_04_06-5	Zu löschendes Key-Objekt ist deaktiviert. (PN_04_08: Deaktivieren eines Key-Objektes)

4.57.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_06-6	Ausführung mit Secure Messaging.

4.57.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_06-7	Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (PN_04_03: Zurücksetzen des Sicherheitszustandes AUTH)

4.57.6 Ablauf

Schritt	Beschreibung						
1	Selektion des DF, in dem das zu löschende Key-Objekt liegt. (PN_04_16: Selektieren eines DF/EF)						
2	DELETE KEY (Übergabe der Key Reference des zu löschenden Key-Objektes)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	e4	21	00	LL	XX...XX	--
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST						

4.57.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des

	Testfalls.

4.58 Testfall: PN_04_07

4.58.1 Informationen

ID	PN_04_07
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Aktivieren eines Key-Objektes
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.58.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.2

4.58.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_07-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_04_07-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_04_07-3	TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_04_07-4	Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (PN_04_02: Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul)

4.58.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_07-5	Ausführung mit Secure Messaging.

4.58.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_07-6	Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (PN_04_03: Zurücksetzen des Sicherheitszustandes AUTH)

4.58.6 Ablauf

Schritt	Beschreibung						
1	Selektion des DF, in dem das zu aktivierende Key-Objekt liegt. (PN_04_16: Selektieren eines DF/EF)						
2	ACTIVATE KEY (Übergabe der Key Reference des zu aktivierenden Key-Objektes)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	44	21	00	LL	XX...XX	--
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.						
	'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST						

4.58.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des

	Testfalls.

4.59 Testfall: PN_04_08

4.59.1 Informationen

ID	PN_04_08
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Deaktivieren eines Key-Objektes
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.59.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.2

4.59.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_08-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_04_08-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_04_08-3	TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_04_08-4	Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (PN_04_02: Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul)

4.59.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_08-5	Ausführung mit Secure Messaging.

4.59.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_08-6	Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (PN_04_03: Zurücksetzen des Sicherheitszustandes AUTH)

4.59.6 Ablauf

Schritt	Beschreibung						
1	Selektion des DF, in dem das zu deaktivierende Key-Objekt liegt. (PN_04_16: Selektieren eines DF/EF)						
2	DEACTIVATE KEY (Übergabe der Key Reference des zu deaktivierenden Key-Objektes)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	04	21	00	LL	XX...XX	--
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Key-Daten inkl. der Key-Reference: a) Für Public Key-Objekt: 'A4-LA4-(83-L83-Key Reference)', Public Key für AT 'B6-LB6-(83-L83-Key Reference)', Public Key für DST b) Für Key Pair-Objekt: 'A4-LA4-(84-01-Key Reference)', Key Pair für AT 'B6-LB6-(84-01-Key Reference)', Key Pair für DST						

4.59.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-

	Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.60 Testfall: PN_04_09a

4.60.1 Informationen

ID	PN_04_09a
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Generierung eines ECC-Schlüsselpaares
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.60.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.2

4.60.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_09a-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_04_09a-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_04_09a-3	TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_04_09a-4	Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (PN_04_02: Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul)

CN-PN_04_09a-5	Key Pair-Objekt, das mit Schlüsseldaten befüllt werden soll, ist im Sicherheitsmodul vorhanden. Ggf. (PN_04_05: Anlegen eines Key-Objektes)
CN-PN_04_09a-6	Falls ein bereits gefülltes Key Pair-Objekt mit neuen Schlüsseldaten befüllt werden soll: Key-Attribut Key-LifeCycleStatus des Key Pair-Objektes besitzt den Wert „operational state – deactivated“. Ggf. (PN_04_08: Deaktivieren eines Key-Objektes)

4.60.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_09a-7	Anwendung insbesondere für die Generierung der GW-Betriebsschlüsselpaare: • Betriebs-TLS-Key Pair (GW_WAN_TLS_PRV, GW_WAN_TLS_PUB) • Betriebs-SIG-Key Pair (GW_WAN_SIG_PRV, GW_WAN_SIG_PUB) • Betriebs-ENC-Key Pair (GW_WAN_ENC_PRV, GW_WAN_ENC_PUB)
CN-PN_04_09a-8	Je nach verwendeter Kommando-Variante des Kommandos GENERATE ASYMMETRIC KEY PAIR erfolgt eine Schlüsselgenerierung mit oder ohne Ausgabe des Public Key.
CN-PN_04_09a-9	Bei der Schlüsselgenerierung ist im Hinblick auf UC_PN_04_12: Use Case „Erstellung eines Zertifikatsrequest-Pakets (SM-PKI)“ darauf zu achten, dass für die äußere Signatur des Zertifikatsrequest-Pakets der alte Signaturschlüssel GW_WAN_SIG_PRV benötigt wird und dieser daher bei der Schlüsselgenerierung nicht überschrieben werden darf.
CN-PN_04_09a-10	Ausführung mit Secure Messaging.

4.60.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_09a-11	Das Key-Attribut Key-LifeCycleStatus des Key Pair-Objektes besitzt nach der Schlüsselgenerierung den Wert „operational state – activated“, so dass das Key Pair-Objekt direkt zu seiner Nutzung für Krypto-Operationen bereitsteht.
CN-PN_04_09a-12	Sofern im Rahmen der Kommando-Ausführung des Kommandos GENERATE ASYMMETRIC KEY PAIR keine Ausgabe des Public Key-Parts des generierten Schlüsselpaares erfolgt, kann ein späterer Export des

	Public Key-Parts über: (PN_04_10: Export des Public Key eines ECC-Schlüsselpaars)
CN-PN_04_09a-13	Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (PN_04_03: Zurücksetzen des Sicherheitszustandes AUTH)

4.60.6 Ablauf

Schritt	Beschreibung														
1	Selektion des DF, in dem das zu deaktivierende Key-Objekt liegt. (PN_04_16: Selektieren eines DF/EF)														
2	GENERATE ASYMMETRIC KEY PAIR: Schlüsselgenerierung mit Ausgabe des Public Key (Übergabe relevanter Informationen für die Schlüsselgenerierung gemäß Kommando-Spezifikation)														
	<table><tr><th>CLA</th><th>INS</th><th>P1</th><th>P2</th><th>Lc</th><th>Data</th><th>Le</th></tr><tr><td>00</td><td>47</td><td>82</td><td>00</td><td>LL</td><td>XX...XX</td><td>XX</td></tr></table>	CLA	INS	P1	P2	Lc	Data	Le	00	47	82	00	LL	XX...XX	XX
	CLA	INS	P1	P2	Lc	Data	Le								
	00	47	82	00	LL	XX...XX	XX								
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.														
'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.															
'Le' enthält die Anzahl der zu erwartenden Oktette.															

4.60.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.61 Testfall: PN_04_10

4.61.1 Informationen

ID	PN_04_10
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Export des Public Key eines ECC-Schlüsselpaars
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.61.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.2

4.61.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_10-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_04_10-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_04_10-3	TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_04_10-4	Key Pair-Objekt, dessen Public Key ausgegeben werden soll, ist im Sicherheitsmodul vorhanden und wurde mittels Schlüsselgenerierung über das Kommando GENERATE ASYMMETRIC KEY PAIR mit Schlüsseldaten befüllt. (PN_04_09: Generierung eines ECC-Schlüsselpaars)

4.61.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_10-5	Anwendung insbesondere für den Export der GW-Betriebsschlüssel (nur Public Key): • Betriebs-TLS-Public Key GW_WAN_TLS_PUB • Betriebs-SIG-Public Key GW_WAN_SIG_PUB • Betriebs-ENC-Public Key GW_WAN_ENC_PUB
CN-PN_04_10-6	Ausführung mit Secure Messaging.

4.61.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.61.6 Ablauf

Schritt	Beschreibung						
1	Selektion des DF, in dem das Key Pair-Objekt liegt, dessen Public Key ausgegeben werden soll. (PN_04_16: Selektieren eines DF/EF)						
2	GENERATE ASYMMETRIC KEY PAIR: Ausgabe des Public Key ohne Schlüsselgenerierung (Übergabe der Key Reference des Key Pair-Objektes, dessen Public Key ausgegeben werden soll)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	47	83	00	LL	XX...XX	XX
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.						
	'Data' enthält die Daten: 'B6-LB6-CRTTemplate', wobei CRTTemplate = Template mit Referenz auf das Key Pair-Objekt (Tag '84'), das dem auszugebenden Public Key zugeordnet ist						
	'Le' enthält die Anzahl der zu erwartenden Oktette.						

4.61.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-

	Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.62 Testfall: PN_04_11

4.62.1 Informationen

ID	PN_04_11
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Import eines Public Key
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.62.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.2

4.62.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_11-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_04_11-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_04_11-3	TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_04_11-4	Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (PN_04_02: Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul)

CN-PN_04_11-5	SIG-Key Pair (GWADM_SIG_PRV, GWADM_SIG_PUB) des GW-Administrators existiert, und der Signaturprüfsschlüssel GWADM_SIG_PUB liegt im Sicherheitsmodul vor und ist aktiviert (ggf. UC_PN_04_07: Use Case „Aktivieren eines Key-Objektes“). (Der initiale Import des GWADM_SIG_PUB erfolgt über die „Initiale Konfigurationsdatei“ im Rahmen der Phase „Vor-Personalisierung + Integration von Sicherheitsmodul und GW“, siehe Kap. 2.5. Für das spätere Einbringen neuer Public Keys GWADM_SIG_PUB_neu in den Phasen „Personalisierung des SMGW“ und „Normalbetrieb des SMGW“ erfolgt eine Nutzung des vorliegenden Use Case „Import eines Public Key“. In letzterem Fall wird als Schlüsselpaar des GW-Administrators zur Sicherung des Schlüsselimports das alte Schlüsselpaar (GWADM_SIG_PRV_alt, GWADM_SIG_PUB_alt) verwendet.)
CN-PN_04_11-6	Zu importierender Public Key KEY_PUB liegt vor. Import-Zertifikat KEY_PUB_CRT zu KEY_PUB liegt vor. Das Import-Zertifikat beinhaltet KEY_PUB (und weitere Key-Zusatzinformationen) und ist vom GW-Administrator mit seinem Signaturschlüssel GWADM_SIG_PRV signiert. Im Falle eines KEY_PUB, der in der SM-PKI zertifiziert ist, entnimmt der GW-Administrator KEY_PUB aus dem zugehörigen Zertifikat der SM-PKI und generiert zu diesem Public Key das vorgenannte Import-Zertifikat. Für die Übereinstimmung der Schlüsseldaten zwischen dem Zertifikat der SM-PKI und dem Import-Zertifikat ist dabei Sorge zu tragen.
CN-PN_04_11-7	Public Key-Objekt zur Speicherung von KEY_PUB ist im Sicherheitsmodul vorhanden. Hierzu Anwendung von UC_PN_04_05: Use Case „Anlegen eines Key-Objektes“ für die Anlage eines Public Key-Objektes für den zu importierenden Public Key, sofern nicht ein bereits vorhandenes Public Key-Objekt mit dem zu importierenden Public Key (neu) befüllt werden soll; bei Neu-Befüllung eines bereits vorhandenen Public Key-Objektes besitzt dabei das Key-Attribut Key-LifeCycleStatus des Public Key-Objektes den Wert „initialisation“ oder „operational state – deactivated“ (UC_PN_04_08: Use Case „Deaktivieren eines Key-Objektes“). Der im Key-Attribut Key-Name des Public Key-Objektes eingetragene Key-Name stimmt mit der Key Reference im Import-Zertifikat zu KEY_PUB überein.

4.62.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_11-8	Besteht für den Use Case zusätzlich der Wunsch nach einer Prüfung des Zertifikates zum zu importierenden Public Key inklusive einer Prüfung seiner Zertifikatskette (im Rahmen der SM-PKI), so ist UC_PN_04_13: Use Case „Prüfung einer Zertifikatskette (SM-PKI)“ hinzuzuziehen.

CN-PN_04_11-9	Relevantes Schlüsselmaterial: • SIG-Key Pair (GWADM_SIG_PRIV, GWADM_SIG_PUB) des GW-Administrators • Zu importierender Public Key KEY_PUB
CN-PN_04_11-10	Ausführung mit Secure Messaging.

4.62.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_11-11	Das Key-Attribut Key-LifeCycleStatus des Public Key-Objektes für KEY_PUB besitzt nach dem Schlüsselimport den Wert „operational state – activated“, so dass das Public Key-Objekt direkt zu seiner Nutzung für Krypto-Operationen bereitsteht.
CN-PN_04_11-12	Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (PN_04_03: Zurücksetzen des Sicherheitszustandes AUTH)

4.62.6 Ablauf

Schritt	Beschreibung														
1	Selektion des DF, in dem das zu befüllende Public Key-Objekt liegt. (PN_04_16: Selektieren eines DF/EF)														
2	MSE SET (DST): Signatur- und Zertifikatverifikation (Übergabe der Key Reference des Public Key-Objektes mit dem Signaturprüfchlüssel GWADM_SIG_PUB und Übergabe des zu verwendenden Krypto-Algorithmus)														
	<table><tr><th>CLA</th><th>INS</th><th>P1</th><th>P2</th><th>Lc</th><th>Data</th><th>Le</th></tr><tr><td>00</td><td>22</td><td>81</td><td>b6</td><td>LL</td><td>XX...XX</td><td>--</td></tr></table>	CLA	INS	P1	P2	Lc	Data	Le	00	22	81	b6	LL	XX...XX	--
	CLA	INS	P1	P2	Lc	Data	Le								
	00	22	81	b6	LL	XX...XX	--								
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.														
'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus) '83-L83-Key Reference' (für das Public Key-Objekt)															
3	PSO VERIFY CERTIFICATE (Übergabe des Import-Zertifikates KEY_PUB_CRT des zu importierenden Public Key KEY_PUB; das Import-Zertifikat enthält insbesondere Key-Zusatzinformationen sowie die Key Reference des zu befüllenden Public Key-Objektes)														

	CLA	INS	P1	P2	Lc	Data	Le
	00	2a	00	be	LL	XX...XX	--
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Daten: Certificate: '7F4E-L7F4E-CertificateBody 5F37-L5F37-Signature' wobei CertificateBody = '5F29-L5F29-CPI 7F49-L7F49- 06-L06-OIDCurve 86-L86-PubKeyWert 5F20-L5F20-KeyName' zu verifizierender Body des Zertifikates, wobei CPI = Certificate Profile Identifier (hier: '71'), OIDCurve = OID der Ellipt. Kurve, PubKeyWert = Schlüsseldaten des Public Key, KeyName = Key-Name des zu füllenden Public Key-Objektes Signature = 'R S' zu verifizierende Signatur über CertificateBody inklusive Tag und Length (entsprechend [TR-03110-3])						

4.62.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.63 Testfall: PN_04_12

4.63.1 Informationen

ID	PN_04_12
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Erstellung eines Zertifikatsrequest-Pakets (SM-PKI)
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.63.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.2

4.63.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_12-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_04_12-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_04_12-3	TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_04_12-4	Altes SIG-Schlüsselpaar (GW_WAN_SIG_PRV_alt, GW_WAN_SIG_PUB_alt) des GW liegt im Sicherheitsmodul vor und ist aktiviert. (PN_03_02: Wechsel der GW-System-PIN, PN_04_09: Generierung eines ECC-Schlüsselpaares, PN_04_07: Aktivieren eines Key-Objektes)
CN-PN_04_12-5	Neue GW-Schlüsselpaare (GW_WAN_TLS_PRV_neu, GW_WAN_TLS_PUB_neu), (GW_WAN_SIG_PRV_neu, GW_WAN_SIG_PUB_neu) bzw. (GW_WAN_ENC_PRV_neu, GW_WAN_ENC_PUB_neu) wurden generiert und sind aktiviert. (PN_04_09: Generierung eines ECC-Schlüsselpaares, PN_04_07: Aktivieren eines Key-Objektes)

4.63.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_12-6	Betrachtet wird hier nur die Erstellung eines Zertifikatsrequest-Pakets für das GW im Rahmen der SM-PKI. Für Details siehe [TR-03109-4].
CN-PN_04_12-7	Anwendung für das Zertifikatsrequest-Paket mit seinen drei Zertifikatsrequests zu neu generierten GW-Betriebsschlüsselpaaren: • Betriebs-TLS-Key Pair (GW_WAN_TLS_PRV_neu, GW_WAN_TLS_PUB_neu) • Betriebs-SIG-Key Pair (GW_WAN_SIG_PRV_neu, GW_WAN_SIG_PUB_neu) • Betriebs-ENC-Key Pair (GW_WAN_ENC_PRV_neu, GW_WAN_ENC_PUB_neu)
CN-PN_04_12-8	Für die äußere Signatur des Zertifikatsrequest-Pakets wird das alte Signaturschlüsselpaar (GW_WAN_SIG_PRV_alt, GW_WAN_SIG_PUB_alt) des GW herangezogen. Beim Wechsel von den vorläufigen GW-Schlüsselpaaren zu den GW-Betriebsschlüsselpaaren im

	Rahmen der Teilphase „Personalisierung des SMGW“ bedeutet dies die Verwendung des vorläufigen GW-Signaturschlüsselpaars für die äußere Signatur des Zertifikatsrequest-Pakets.
CN-PN_04_12-9	Die Generierung der Autorisierungssignatur zum Zertifikatsrequest-Paket liegt außerhalb des vorliegenden Use Case.
CN-PN_04_12-10	Ausführung mit Secure Messaging.

4.63.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.63.6 Ablauf

Schritt	Beschreibung
1	Sofern für das neue Schlüsselpaar (GW_WAN_TLS_PRV_neu, GW_WAN_TLS_PUB_neu) in UC_PN_04_09: Use Case „Generierung eines ECC-Schlüsselpaars“ keine Ausgabe des Public Key-Parts erfolgt ist, für den Export des Public Key GW_WAN_TLS_PUB_neu Durchführung von (PN_04_10: Export des Public Key eines ECC-Schlüsselpaars)
2	Zusammenstellung des Zertifikatsrequests zum Public Key GW_WAN_TLS_PUB_neu. Ergebnis: ZertRequest_TLS.
3	Für die innere Signatur des Zertifikatsrequests: Aufbereitung von ZertRequest_TLS für die innere Signatur (Hashing). Ergebnis: InputSig_ZertRequest_TLS.
4	Für die innere Signatur des Zertifikatsrequests: mit InputSig_ZertRequest_TLS als Signaturdaten und unter Nutzung von GW_WAN_TLS_PRV_neu als Signaturschlüssel (→ „Selbst-Signatur des neuen TLS-Schlüssels“) und mit Ergebnis: Sig_ZertRequest_TLS Durchführung von (PN_05_02: Generieren einer Signatur / DST)
5	Zusammenstellung des finalen Zertifikatsrequests zum TLS-Schlüsselpaar, bestehend aus ZertRequest_TLS und Sig_ZertRequest_TLS.
6	Sofern für das neue Schlüsselpaar (GW_WAN_SIG_PRV_neu, GW_WAN_SIG_PUB_neu) in UC_PN_04_09: Use Case „Generierung eines ECC-Schlüsselpaars“ keine Ausgabe des Public Bundesamt für Sicherheit in der Informationstechnik 57 4 Personalisierung, Normalbetrieb (End-Usage) und Außerbetriebnahme des SMGW Key-Parts erfolgt ist, für den Export des Public Key GW_WAN_SIG_PUB_neu Durchführung von (PN_04_10: Export des Public Key eines ECC-Schlüsselpaars)

7	Zusammenstellung des Zertifikatsrequests zum Public Key GW_WAN_SIG_PUB_neu. Ergebnis: ZertRequest_SIG.
8	Für die innere Signatur des Zertifikatsrequests: Aufbereitung von ZertRequest_SIG für die innere Signatur (Hashing). Ergebnis: InputSig_ZertRequest_SIG
9	Für die innere Signatur des Zertifikatsrequests: mit InputSig_ZertRequest_SIG als Signaturdaten und unter Nutzung von GW_WAN_SIG_PRV_neu als Signaturschlüssel (→ „Selbst-Signatur des neuen SIG-Schlüssels“) und mit Ergebnis: Sig_ZertRequest_SIG: (PN_05_02: Generieren einer Signatur / DST)
10	Zusammenstellung des finalen Zertifikatsrequests zum SIG-Schlüsselpaar, bestehend aus ZertRequest_SIG und Sig_ZertRequest_SIG.
11	Sofern für das neue Schlüsselpaar (GW_WAN_ENC_PRV_neu, GW_WAN_ENC_PUB_neu) in UC_PN_04_09: Use Case „Generierung eines ECC- Schlüsselpaares“ keine Ausgabe des Public Key-Parts erfolgt ist, für " + "den Export des Public Key GW_WAN_ENC_PUB_neu Durchführung von (PN_04_10: Export des Public Key eines ECC-Schlüsselpaares)
12	Zusammenstellung des Zertifikatsrequests zum Public Key GW_WAN_ENC_PUB_neu. Ergebnis: ZertRequest_ENC.
13	Für die innere Signatur des Zertifikatsrequests: Aufbereitung von ZertRequest_ENC für die innere Signatur (Hashing). Ergebnis: InputSig_ZertRequest_ENC.
14	Für die innere Signatur des Zertifikatsrequests: mit InputSig_ZertRequest_ENC als Signaturdaten und unter Nutzung von GW_WAN_ENC_PRV_neu als Signaturschlüssel (→ „Selbst-Signatur des neuen ENC-Schlüssels“) und mit Ergebnis: Sig_ZertRequest_ENC Durchführung von (PN_05_03: Generieren einer Signatur / AT)
15	Zusammenstellung des finalen Zertifikatsrequests zum ENC-Schlüsselpaar, bestehend aus ZertRequest_ENC und Sig_ZertRequest_ENC.
16	Erstellung des Zertifikatsrequest-Pakets, bestehend aus • ZertRequest_TLS und Sig_ZertRequest_TLS • ZertRequest_SIG und Sig_ZertRequest_SIG • ZertRequest_ENC und Sig_ZertRequest_ENC Ergebnis: ZertRequestPaket.
17	Für die äußere Signatur des Zertifikatsrequest-Pakets: Aufbereitung von ZertRequestPaket für die äußere Signatur (Hashing). Ergebnis: InputSig_ZertRequestPaket.
18	Für die äußere Signatur des Zertifikatsrequest-Pakets: mit InputSig_ZertRequestPaket als Signaturdaten und unter Nutzung von GW_WAN_SIG_PRV_alt als Signaturschlüssel und mit Ergebnis: Sig_ZertRequestPaket: (PN_05_02: Generieren einer Signatur / DST)
19	Zusammenstellung des finalen Zertifikatsrequest-Pakets zu den drei neuen

	Schlüsselpaaren, bestehend aus ZertRequestPaket und Sig_ZertRequestPaket.

4.63.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.64 Testfall: PN_04_13

4.64.1 Informationen

ID	PN_04_13
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Prüfung einer Zertifikatskette (SM-PKI)
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.64.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.2

4.64.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_13-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_04_13-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)

CN-PN_04_13-3	TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_04_13-4	Kette der zu prüfenden Zertifikate (bis ggf. auf das SM-PKI-Root-Zertifikat) liegt im GW vor.
CN-PN_04_13-5	Der Root-Public Key der SM-PKI liegt im Sicherheitsmodul vor und ist aktiviert. Der im Sicherheitsmodul im Public Key-Objekt Key.SMPKIRoot_x gespeicherte Root-Public Key stimmt mit dem Public Key des SM-PKI-Root-Zertifikates, das im zum Root-Public Key zugehörigen Datenfeld EF.SMPKIRoot_x im Sicherheitsmodul abgelegt ist, überein.

4.64.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_13-6	Betrachtet wird hier nur die Prüfung einer Kette von X.509-Zertifikaten bis zur SM-PKI-Root im Rahmen der SM-PKI. Für Details siehe [TR-03109-4].
CN-PN_04_13-7	Die Prüfung einer Zertifikatskette baut auf der Prüfung einzelner (Zertifikats-) Signaturen auf. Für das Parsen der beteiligten X.509-Zertifikate ist das GW zuständig.
CN-PN_04_13-8	Für den Use Case wird angenommen, dass das SM-PKI-Root-Zertifikat im transparenten Datenfeld EF.SMPKIRoot_x im DF.SMGW und der Root-Public Key des Zertifikates im zugehörigen Public Key-Objekt Key.SMPKIRoot_x im DF.SMGW gespeichert ist.
CN-PN_04_13-9	Ausführung mit Secure Messaging.

4.64.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.64.6 Ablauf

Schritt	Beschreibung
1	Fortlaufende Anwendung von UC_PN_05_02: Use Case „Prüfen einer Signatur / DST“. Für die einzelnen zu prüfenden Zertifikate ist jeweils der Zertifikatsbody und

	die Signatur des Zertifikates Bundesamt für Sicherheit in der Informationstechnik 59 4 Personalisierung, Normalbetrieb (End-Usage) und Außerbetriebnahme des SMGW aus dem Zertifikat zu extrahieren sowie der relevante Signaturprüfchlüssel zu bestimmen und ggf. dieser Signaturprüfchlüssel in das Sicherheitsmodul zu importieren (Übergabe des Signaturprüfchlüssels im Kommando PSO VERIFY DIGITAL SIGNATURE oder Anwendung von UC_PN_04_11: Use Case „Import eines Public Key“), falls der Signaturprüfchlüssel nicht anderweitig schon im Sicherheitsmodul vorliegt.
2	Für die Prüfung gegen das SM-PKI-Root-Zertifikat: Signaturprüfchlüssel ist der im Sicherheitsmodul im Public Key-Objekt Key.SMPKIRoot_x hinterlegte Root-Public Key (der mit dem Public Key des SM-PKI-Root-Zertifikates, das im zugehörigen Datenfeld EF.SMPKIRoot_x abgelegt ist, übereinstimmt).

4.64.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.65 Testfall: PN_04_14a

4.65.1 Informationen

ID	PN_04_14a
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Prüfung einer Zertifikatskette (SM-PKI)
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.65.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.3

4.65.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_14a-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_04_14a-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_04_14a-3	TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_04_14a-4	Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (PN_04_02: Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul)
CN-PN_04_14a-5	Zu schreibendes neues SM-PKI-Root-Zertifikat inkl. des zugehörigen Link-Zertifikates liegt vor.

4.65.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_14a-6	Die Speicherung des neuen SM-PKI-Root-Zertifikates erfolgt im transparenten Datenfeld EF.SMPKIRoot_x im DF.SMGW. Ferner erfolgt die Speicherung des neuen Root-Public Key aus dem neuen SM-PKI-Root-Zertifikat im vorgesehenen zugehörigen Public Key-Objekt Key.SMPKIRoot_x im DF.SMGW. Die zusätzliche Speicherung des Root-Public Key aus dem Zertifikat erfolgt aus dem Grund, als dass das Sicherheitsmodul bei Krypto-Operationen mit dem Root-Public Key mit diesem nur in Form eines Public Key-Objektes arbeiten und hierfür nicht auf den im Zertifikat enthaltenen Public Key zurückgreifen kann.
CN-PN_04_14a-7	Bzgl. der Speicherung des neuen Root-Public Key im Sicherheitsmodul hat der GW-Administrator für die Übereinstimmung zwischen dem Public Key im Zertifikat und dem importierten Public Key Sorge zu tragen.
CN-PN_04_14a-8	Beim Update des SM-PKI-Root-Zertifikates ist zu beachten, dass ein Überschreiben des aktuell gespeicherten alten SM-PKI-Root-Zertifikates aus Anwendungssicht evtl. nicht erwünscht ist. Entsprechendes gilt für das Update des zugehörigen Root-Public Key aus dem Zertifikat bzw. das zugehörige Public Key-Objekt mit den Schlüsseldaten des alten Root-

	Public Key.
CN-PN_04_14a-9	Ausführung mit Secure Messaging.

4.65.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_14a-10	Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (PN_04_03: Zurücksetzen des Sicherheitszustandes AUTH)

4.65.6 Ablauf

Schritt	Beschreibung						
1	Prüfung des Link-Zertifikates unter Nutzung von UC_PN_05_04: Use Cases „Prüfen einer Signatur / DST“. Aus dem Link-Zertifikat ist der Zertifikatsbody und die Signatur des Zertifikates zu extrahieren; ferner ist der relevante Signaturprüf Schlüssel (hier: der alte Root-Public Key) zu bestimmen. Zu prüfen ist die Signatur über den Zertifikatsbody des Link-Zertifikates unter Nutzung dieses Signaturprüf Schlüssels.						
2	Selektion des DF.SMGW. (PN_04_16: Selektieren eines DF/EF)						
3	SELECT: EF (File-ID des EF.SMPKIRoot_x)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	a4	02	0c	02	XX XX	--
	'Data' enthält den File-Identifizier des zu selektierenden EF.						
4	UPDATE BINARY (SM-PKI-Root-Zertifikat)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	d6	XX	XX	LL	XX...XX	--
	'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}.						
'P2' enthält den Offset mod 256.							
'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.							
'Data' enthält die zu schreibenden neuen Daten.							

5	Extrahieren des Root-Public Key aus dem SM-PKI-Root-Zertifikat.
6	Für den Import des neuen Root-Public Key in das Sicherheitsmodul und die Speicherung des neuen Root-Public Key im dafür vorgesehenen Public Key-Objekt Key.SMPKIRoot_x Durchführung von (PN_04_11: Import eines Public Key)

4.65.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.66 Testfall: PN_04_14b

4.66.1 Informationen

ID	PN_04_14b
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Prüfung einer Zertifikatskette (SM-PKI)
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.66.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.3

4.66.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_14b-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

CN-PN_04_14b-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_04_14b-3	TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_04_14b-4	Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (PN_04_02: Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul)
CN-PN_04_14b-5	Zu schreibendes neues SM-PKI-Root-Zertifikat inkl. des zugehörigen Link-Zertifikates liegt vor.

4.66.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_14b-6	Die Speicherung des neuen SM-PKI-Root-Zertifikates erfolgt im transparenten Datenfeld EF.SMPKIRoot_x im DF.SMGW. Ferner erfolgt die Speicherung des neuen Root-Public Key aus dem neuen SM-PKI-Root-Zertifikat im vorgesehenen zugehörigen Public Key-Objekt Key.SMPKIRoot_x im DF.SMGW. Die zusätzliche Speicherung des Root-Public Key aus dem Zertifikat erfolgt aus dem Grund, als dass das Sicherheitsmodul bei Krypto-Operationen mit dem Root-Public Key mit diesem nur in Form eines Public Key-Objektes arbeiten und hierfür nicht auf den im Zertifikat enthaltenen Public Key zurückgreifen kann.
CN-PN_04_14b-7	Bzgl. der Speicherung des neuen Root-Public Key im Sicherheitsmodul hat der GW-Administrator für die Übereinstimmung zwischen dem Public Key im Zertifikat und dem importierten Public Key Sorge zu tragen.
CN-PN_04_14b-8	Beim Update des SM-PKI-Root-Zertifikates ist zu beachten, dass ein Überschreiben des aktuell gespeicherten alten SM-PKI-Root-Zertifikates aus Anwendungssicht evtl. nicht erwünscht ist. Entsprechendes gilt für das Update des zugehörigen Root-Public Key aus dem Zertifikat bzw. das zugehörige Public Key-Objekt mit den Schlüsseldaten des alten Root-Public Key.
CN-PN_04_14b-9	Ausführung mit Secure Messaging.

4.66.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_14b-10	Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (PN_04_03: Zurücksetzen des Sicherheitszustandes AUTH)

4.66.6 Ablauf

Schritt	Beschreibung														
1	Prüfung des Link-Zertifikates unter Nutzung von UC_PN_05_04: Use Cases „Prüfen einer Signatur / DST“. Aus dem Link-Zertifikat ist der Zertifikatsbody und die Signatur des Zertifikates zu extrahieren; ferner ist der relevante Signaturprüfchlüssel (hier: der alte Root-Public Key) zu bestimmen. Zu prüfen ist die Signatur über den Zertifikatsbody des Link-Zertifikates unter Nutzung dieses Signaturprüfchlüssels.														
2	Selektion des DF.SMGW. (PN_04_16: Selektieren eines DF/EF)														
3	UPDATE BINARY (SFI des EF.SMPKIRoot_x, SM-PKI-Root-Zertifikat)														
	<table><tr><th>CLA</th><th>INS</th><th>P1</th><th>P2</th><th>Lc</th><th>Data</th><th>Le</th></tr><tr><td>00</td><td>d6</td><td>XX</td><td>XX</td><td>LL</td><td>XX...XX</td><td>--</td></tr></table>	CLA	INS	P1	P2	Lc	Data	Le	00	d6	XX	XX	LL	XX...XX	--
	CLA	INS	P1	P2	Lc	Data	Le								
	00	d6	XX	XX	LL	XX...XX	--								
	'P1' enthält '80' + SFI.														
'P2' enthält den Offset aus {'00', ..., 'FF'}.															
'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.															
'Data' enthält die zu schreibenden neuen Daten.															
4	Extrahieren des Root-Public Key aus dem SM-PKI-Root-Zertifikat.														
5	Für den Import des neuen Root-Public Key in das Sicherheitsmodul und die Speicherung des neuen Root-Public Key im dafür vorgesehenen Public Key-Objekt Key.SMPKIRoot_x Durchführung von (PN_04_11: Import eines Public Key)														

4.66.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.67 Testfall: PN_04_15a

4.67.1 Informationen

ID	PN_04_15a
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Auslesen des SM-PKI-Root-Zertifikates
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.67.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.3

4.67.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_15a-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_04_15a-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_04_15a-3	TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)

4.67.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_15a-4	Die Speicherung des SM-PKI-Root-Zertifikates erfolgt im transparenten Datenfeld EF.SMPKIRoot_x im DF.SMGW.

CN-PN_04_15a-5	Für das Parsen des X.509-Zertifikates ist das GW zuständig.
CN-PN_04_15a-6	Ausführung mit Secure Messaging.

4.67.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.67.6 Ablauf

Schritt	Beschreibung						
1	Selektion des DF.SMGW. (PN_04_16: Selektieren eines DF/EF)						
2	SELECT: EF (File-ID des EF.SMPKIRoot_x)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	a4	02	0c	02	XX XX	--
	'Data' enthält den File-Identifizier des zu selektierenden EF.						
3	READ BINARY						
	CLA	INS	P1	P2	Lc	Data	Le
	00	b0	XX	XX	--	--	XX
	'P1' enthält (Offset - P2) / 256, wobei Offset aus {'0000', ..., '7FFF'}. 'P2' enthält den Offset mod 256. 'Le' enthält die Anzahl der zu erwartenden Oktette.						

4.67.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.68 Testfall: PN_04_15b

4.68.1 Informationen

ID	PN_04_15b
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Auslesen des SM-PKI-Root-Zertifikates
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.68.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.3

4.68.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_15b-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_04_15b-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_04_15b-3	TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)

4.68.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_15b-4	Die Speicherung des SM-PKI-Root-Zertifikates erfolgt im transparenten Datenfeld EF.SMPKIRoot_x im DF.SMGW.

CN-PN_04_15b-5	Für das Parsen des X.509-Zertifikates ist das GW zuständig.
CN-PN_04_15b-6	Ausführung mit Secure Messaging.

4.68.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.68.6 Ablauf

Schritt	Beschreibung						
1	Selektion des DF.SMGW. (PN_04_16: Selektieren eines DF/EF)						
2	READ BINARY (SFI des EF.SMPKIRoot_x)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	b0	XX	XX	--	--	XX
	'P1' enthält '80' + SFI. 'P2' enthält den Offset aus {'00', ..., 'FF'}. 'Le' enthält die Anzahl der zu erwartenden Oktette.						

4.68.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.69 Testfall: PN_04_16a

4.69.1 Informationen

ID	PN_04_16a
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Selektieren eines DF/EF

Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.69.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.4

4.69.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_16a-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

4.69.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_16a-2	Die Selektion eines DF/EF per File-ID erfolgt innerhalb des aktuell selektierten DF. Um im Filesystem des Sicherheitsmoduls zu navigieren, ist ggf. eine sukzessive mehrfache Anwendung des Use Cases „Selektieren eines DF/EF“ erforderlich.
CN-PN_04_16a-3	Das DF.SMGW kann auch direkt per AID selektiert werden.
CN-PN_04_16a-4	Beim Hochfahren des Sicherheitsmoduls ist automatisch das MF selektiert.
CN-PN_04_16a-5	Ausführung ohne Secure Messaging.

4.69.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.69.6 Ablauf

Schritt	Beschreibung						
1	SELECT: MF (leeres Kommando-Datenfeld)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	a4	00	0c	02	3f 00	--

4.69.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.70 Testfall: PN_04_16b

4.70.1 Informationen

ID	PN_04_16b
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Selektieren eines DF/EF
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.70.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.4

4.70.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_16b-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

4.70.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_16b-2	Die Selektion eines DF/EF per File-ID erfolgt innerhalb des aktuell selektierten DF. Um im Filesystem des Sicherheitsmoduls zu navigieren, ist ggf. eine sukzessive mehrfache Anwendung des Use Cases „Selektieren eines DF/EF“ erforderlich.
CN-PN_04_16b-3	Das DF.SMGW kann auch direkt per AID selektiert werden.
CN-PN_04_16b-4	Beim Hochfahren des Sicherheitsmoduls ist automatisch das MF selektiert.
CN-PN_04_16b-5	Ausführung ohne Secure Messaging.

4.70.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.70.6 Ablauf

Schritt	Beschreibung						
1	SELECT: DF (File-ID des zu selektierenden DF)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	a4	01	0c	02	XX XX	--
	'Data' enthält den File-Identifizier des zu selektierenden DF.						

4.70.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des

	Testfalls.

4.71 Testfall: PN_04_16c

4.71.1 Informationen

ID	PN_04_16c
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Selektieren eines DF/EF
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.71.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.4

4.71.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_16c-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

4.71.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_16c-2	Die Selektion eines DF/EF per File-ID erfolgt innerhalb des aktuell selektierten DF. Um im Filesystem des Sicherheitsmoduls zu navigieren, ist ggf. eine sukzessive mehrfache Anwendung des Use Cases „Selektieren eines DF/EF“ erforderlich.
CN-PN_04_16c-3	Das DF.SMGW kann auch direkt per AID selektiert werden.

CN-PN_04_16c-4	Beim Hochfahren des Sicherheitsmoduls ist automatisch das MF selektiert.
CN-PN_04_16c-5	Ausführung ohne Secure Messaging.

4.71.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.71.6 Ablauf

Schritt	Beschreibung						
1	SELECT: EF (File-ID des zu selektierenden EF)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	a4	02	0c	02	XX XX	--
	'Data' enthält den File-Identifizier des zu selektierenden EF.						

4.71.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.72 Testfall: PN_04_16d

4.72.1 Informationen

ID	PN_04_16d
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Selektieren eines DF/EF
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW

Rollen	GW, GW_Administrator

4.72.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.4

4.72.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_16d-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

4.72.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_16d-2	Die Selektion eines DF/EF per File-ID erfolgt innerhalb des aktuell selektierten DF. Um im Filesystem des Sicherheitsmoduls zu navigieren, ist ggf. eine sukzessive mehrfache Anwendung des Use Cases „Selektieren eines DF/EF“ erforderlich.
CN-PN_04_16d-3	Das DF.SMGW kann auch direkt per AID selektiert werden.
CN-PN_04_16d-4	Beim Hochfahren des Sicherheitsmoduls ist automatisch das MF selektiert.
CN-PN_04_16d-5	Ausführung ohne Secure Messaging.

4.72.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.72.6 Ablauf

Schritt	Beschreibung						
1	SELECT: DF (AID des DF.SMGW)						
	CLA	INS	P1	P2	Lc	Data	Le

	00	a4	04	0c	LL	XX...XX	--
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält den Application-Identifizier des zu selektierenden DF.						

4.72.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.73 Testfall: PN_04_17

4.73.1 Informationen

ID	PN_04_17
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Anlegen eines DF/EF
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.73.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.4

4.73.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_17-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_04_17-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und

	Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_04_17-3	TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_04_17-4	Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (PN_04_02: Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul)
CN-PN_04_17-5	Ausgewähltes FILE ist nicht logisch/physikalisch terminiert

4.73.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_17-6	Ausführung mit Secure Messaging.

4.73.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_17-7	Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (PN_04_03: Zurücksetzen des Sicherheitszustandes AUTH)

4.73.6 Ablauf

Schritt	Beschreibung						
1	Selektion des DF, in dem das neue DF/EF angelegt werden soll. (PN_04_16: Selektieren eines DF/EF)						
2	CREATE FILE (Übergabeparameter gemäß Kommando-Spezifikation)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	e0	00	00	LL	XX...XX	XX

	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Oktette mit den Spezifikationsparametern für das anzulegende File. 'Le' enthält die Anzahl der zu erwartenden Oktette.

4.73.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.74 Testfall: PN_04_18a

4.74.1 Informationen

ID	PN_04_18a
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Löschen eines DF/EF
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.74.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.4

4.74.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_18a-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_04_18a-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im

	Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_04_18a-3	TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_04_18a-4	Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (PN_04_02: Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul)
CN-PN_04_18a-5	Ausgewähltes FILE ist nicht logisch/physikalisch terminiert

4.74.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_18a-6	Ausführung mit Secure Messaging.

4.74.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_18a-7	Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (PN_04_03: Zurücksetzen des Sicherheitszustandes AUTH)

4.74.6 Ablauf

Schritt	Beschreibung						
1	Selektion des DF, in dem das zu löschende DF/EF liegt. (PN_04_16: Selektieren eines DF/EF)						
2	SELECT: DF (File-ID des zu löschenden DF/EF)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	a4	01	0c	02	XX XX	--
	'Data' enthält den File-Identifizier des zu selektierenden DF.						

3	DELETE FILE						
	CLA	INS	P1	P2	Lc	Data	Le
	00	e4	00	00	--	--	--

4.74.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.75 Testfall: PN_04_19a

4.75.1 Informationen

ID	PN_04_19a
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Aktivieren eines DF/EF
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.75.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.4

4.75.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_19a-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"

CN-PN_04_19a-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_04_19a-3	TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_04_19a-4	Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (PN_04_02: Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul)
CN-PN_04_19a-5	Ausgewähltes FILE ist nicht logisch/physikalisch terminiert

4.75.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_19a-6	Ausführung mit Secure Messaging.

4.75.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_19a-7	Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (PN_04_03: Zurücksetzen des Sicherheitszustandes AUTH)

4.75.6 Ablauf

Schritt	Beschreibung						
1	Selektion des DF, in dem das zu aktivierende DF/EF liegt. (PN_04_16: Selektieren eines DF/EF)						
2	SELECT: DF (File-ID des zu aktivierenden DF/EF)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	a4	01	0c	02	XX XX	--

	'Data' enthält den File-Identifizier des zu selektierenden DF.						
3	ACTIVATE FILE						
	CLA	INS	P1	P2	Lc	Data	Le
	00	44	00	00	--	--	--

4.75.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.76 Testfall: PN_04_20a

4.76.1 Informationen

ID	PN_04_20a
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Deaktivieren eines DF/EF
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.76.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.4

4.76.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN-PN_04_20a-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_04_20a-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_04_20a-3	TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_04_20a-4	Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (PN_04_02: Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul)
CN-PN_04_20a-5	Ausgewähltes FILE ist nicht logisch/physikalisch terminiert

4.76.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_20a-6	Ausführung mit Secure Messaging.

4.76.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_20a-7	Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (PN_04_03: Zurücksetzen des Sicherheitszustandes AUTH)

4.76.6 Ablauf

Schritt	Beschreibung						
1	Selektion des DF, in dem das zu aktivierende DF/EF liegt. (PN_04_16: Selektieren eines DF/EF)						
2	SELECT: DF (File-ID des zu aktivierenden DF/EF)						
	CLA	INS	P1	P2	Lc	Data	Le

	00	a4	01	0c	02	XX XX	--
	'Data' enthält den File-Identifizier des zu selektierenden DF.						
3	DEACTIVATE FILE						
	CLA	INS	P1	P2	Lc	Data	Le
	00	04	00	00	--	--	--

4.76.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.77 Testfall: PN_04_21a

4.77.1 Informationen

ID	PN_04_21a
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Terminieren eines DF
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.77.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.4

4.77.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN-PN_04_21a-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_04_21a-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_04_21a-3	TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_04_21a-4	Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (PN_04_02: Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul)
CN-PN_04_21a-5	Ausgewähltes FILE ist nicht logisch/physikalisch terminiert

4.77.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_21a-6	Ausführung mit Secure Messaging.

4.77.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_21a-7	Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (PN_04_03: Zurücksetzen des Sicherheitszustandes AUTH)

4.77.6 Ablauf

Schritt	Beschreibung						
1	Selektion des DF, in dem das zu terminierende DF liegt. (PN_04_16: Selektieren eines DF/EF)						
2	SELECT: DF (File-ID des zu terminierenden DF)						
	CLA	INS	P1	P2	Lc	Data	Le

	00	a4	01	0c	02	XX XX	--
	'Data' enthält den File-Identifizier des zu selektierenden DF.						
3	TERMINATE DF						
	CLA	INS	P1	P2	Lc	Data	Le
	00	e6	00	00	--	--	--

4.77.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.78 Testfall: PN_04_21b

4.78.1 Informationen

ID	PN_04_21b
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Terminieren eines EF
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.78.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.4

4.78.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN-PN_04_21b-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_04_21b-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_04_21b-3	TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_04_21b-4	Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (PN_04_02: Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul)
CN-PN_04_21b-5	Ausgewähltes FILE ist nicht logisch/physikalisch terminiert

4.78.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_21b-6	Ausführung mit Secure Messaging.

4.78.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_21b-7	Sofern durch den GW-Administrator keine weiteren Administrationstätigkeiten am Sicherheitsmodul vorgenommen werden sollen, wird empfohlen, im Sicherheitsmodul den Sicherheitszustand AUTH explizit zurückzusetzen. (PN_04_03: Zurücksetzen des Sicherheitszustandes AUTH)

4.78.6 Ablauf

Schritt	Beschreibung						
1	Selektion des DF, in dem das zu terminierende EF liegt. (PN_04_16: Selektieren eines DF/EF)						
2	SELECT: EF (File-ID des zu terminierenden EF)						
	CLA	INS	P1	P2	Lc	Data	Le

	00	a4	02	0c	02	XX XX	--
	'Data' enthält den File-Identifizier des zu selektierenden EF.						
3	TERMINATE EF						
	CLA	INS	P1	P2	Lc	Data	Le
	00	e8	00	00	--	--	--

4.78.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.79 Testfall: PN_04_22

4.79.1 Informationen

ID	PN_04_22
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Terminieren des Sicherheitsmoduls
Klassifizierung	Gutfall-Test
Phase	Außerbetriebnahme des SMGW
Rollen	GW, GW_Administrator

4.79.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.5

4.79.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN-PN_04_22-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_04_22-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_04_22-3	TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)
CN-PN_04_22-4	Erfolgreiche Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul, d.h. der Sicherheitszustand AUTH ist im Sicherheitsmodul gesetzt. (PN_04_02: Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul)
CN-PN_04_22-5	Ausgewähltes FILE ist nicht logisch/physikalisch terminiert

4.79.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_22-6	Ausführung mit Secure Messaging.

4.79.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_22-7	Erfolgreiche Kommando-Ausführung nimmt das Sicherheitsmodul irreversibel außer Betrieb. Für die nachfolgend noch ausführbaren Kommandos siehe [TR-03109-2], Kap. 3.4.10.1, 4.9.1.

4.79.6 Ablauf

Schritt	Beschreibung						
1	TERMINATE CARD USAGE						
	CLA	INS	P1	P2	Lc	Data	Le
	00	fe	00	00	--	--	--

4.79.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.80 Testfall: PN_04_23

4.80.1 Informationen

ID	PN_04_23
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Terminieren des Sicherheitsmoduls
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, GW_Administrator

4.80.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.4.6

4.80.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_23-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_04_23-2	TLS-Kanal zwischen GW-Administrator und GW besteht. (PN_04_01: Aufbau eines TLS-Kanals zwischen GW-Administrator und SMGW)

4.80.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_23-3	Anwendung zum gezielten Zurücksetzen der Applikationsebene des Sicherheitsmoduls.
CN-PN_04_23-4	Ausführung ohne Secure Messaging.

4.80.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_04_23-5	Das Zurücksetzen der Applikationsebene des Sicherheitsmoduls beinhaltet eine Re-Initialisierung des Sicherheitsmoduls mit Werten, wie diese nach einem Cold- bzw. Warm-Reset des Sicherheitsmoduls gesetzt sind, und ist insbesondere mit dem Zurücksetzen aller Sicherheitszustände (hier: PACE, AUTH), dem Schließen sicherer Kanäle, dem Löschen von Session Keys und der Selektion des MF verbunden. Für nachfolgende Zugriffe auf das Sicherheitsmodul, die einen gesetzten Sicherheitszustand PACE und / oder AUTH erfordern, ist das PACE-Protokoll bzw. die externe Authentisierung des GW-Administrators erneut erfolgreich auszuführen (PN_03_01: PACE-Authentisierung, PN_04_02: Authentisierung des GW-Administrators gegenüber dem Sicherheitsmodul)

4.80.6 Ablauf

Schritt	Beschreibung						
1	MANAGE CHANNEL						
	CLA	INS	P1	P2	Lc	Data	Le
	00	70	40	10	--	--	--

4.80.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.81 Testfall: PN_05_01

4.81.1 Informationen

ID	PN_05_01
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Erzeugen und Ausgeben einer Zufallszahl
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, EXT

4.81.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.5

4.81.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_01-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_05_01-2	Sofern das Kommando GET CHALLENGE mit Secure Messaging ausgeführt werden soll: Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)

4.81.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_01-3	Ausführung des Kommandos GET CHALLENGE mit oder ohne Secure Messaging. Die das Kommando GET CHALLENGE aufrufende Stelle zeigt über das CLA-Byte im Kommando-Header an, ob das Kommando mit oder ohne Secure Messaging ausgeführt werden soll.

4.81.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_01-4	Im Fall der Variante P1='00' steht die generierte Zufallszahl auch Sicherheitsmodul-intern weiterhin zur Verfügung (z.B. für ein nachfolgendes Kommando EXTERNAL AUTHENTICATE); im Fall der Variante P1='01' wird die Zufallszahl nur nach extern ausgegeben.

4.81.6 Ablauf

Schritt	Beschreibung						
1	GET CHALLENGE (Anzeige der gewünschten Länge der Zufallszahl im Kommando)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	84	XX	00	--	--	XX
	'P1' enthält '00': generierte Zufallszahl wird intern gespeichert '01': generierte Zufallszahl wird intern nicht gespeichert. 'Le' enthält die Anzahl der Oktette zu erwartenden Zufallszahl (Hersteller-abhängig und in Abhängigkeit vom Ausgabeformat).						

4.81.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.82 Testfall: PN_05_02

4.82.1 Informationen

ID	PN_05_02
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Generieren einer Signatur / DST

Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, EXT

4.82.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.5

4.82.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_02-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_05_02-2	Sofern das Kommando GET CHALLENGE mit Secure Messaging ausgeführt werden soll: Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_05_02-3	Key Pair-Objekt mit dem Signaturschlüssel ist im Sicherheitsmodul vorhanden und ist aktiviert. (PN_04_09: Generierung eines ECC-Schlüsselpaares, PN_04_07: Aktivieren eines Key-Objektes)

4.82.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_02-4	Die Aufbereitung der zu signierenden Daten inkl. Hashen der Daten erfolgt durch das GW bzw. anderweitig außerhalb des Sicherheitsmoduls (Signaturdaten).
CN-PN_05_02-5	Ausführung mit Secure Messaging.

4.82.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.82.6 Ablauf

Schritt	Beschreibung														
1	Aufbereitung der Signaturdaten inkl. Hashing (passend zur vorgesehenen Elliptischen Kurve / Schlüssellänge des Signaturschlüssels).														
2	Bestimmung des Signaturschlüssels bzw. des zugehörigen Key Pair-Objektes im Sicherheitsmodul (Speicherort im Filesystem, Key-ID). Selektion des DF, in dem der Signaturschlüssel bzw. das zugehörige Key Pair-Objekt liegt. (PN_04_16: Selektieren eines DF/EF)														
3	MSE SET (DST): Signaturerzeugung (Übergabe der Key Reference des Key Pair-Objektes mit dem Signaturschlüssel und Übergabe des zu verwendenden Krypto-Algorithmus)														
	<table><tr><th>CLA</th><th>INS</th><th>P1</th><th>P2</th><th>Lc</th><th>Data</th><th>Le</th></tr><tr><td>00</td><td>22</td><td>41</td><td>b6</td><td>LL</td><td>XX...XX</td><td>--</td></tr></table>	CLA	INS	P1	P2	Lc	Data	Le	00	22	41	b6	LL	XX...XX	--
	CLA	INS	P1	P2	Lc	Data	Le								
	00	22	41	b6	LL	XX...XX	--								
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.														
'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus) '84-01-Key Reference' (für das Key Pair-Objekt)															
4	PSO COMPUTE DIGITAL SIGNATURE (Signaturdaten))														
	<table><tr><th>CLA</th><th>INS</th><th>P1</th><th>P2</th><th>Lc</th><th>Data</th><th>Le</th></tr><tr><td>00</td><td>2a</td><td>9e</td><td>9a</td><td>LL</td><td>XX...XX</td><td>XX</td></tr></table>	CLA	INS	P1	P2	Lc	Data	Le	00	2a	9e	9a	LL	XX...XX	XX
	CLA	INS	P1	P2	Lc	Data	Le								
	00	2a	9e	9a	LL	XX...XX	XX								
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.														
'Data' enthält die zu signierende Daten als Oktett-String.															
'Le' enthält die Anzahl der zu erwartenden Oktette.															

4.82.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.83 Testfall: PN_05_03

4.83.1 Informationen

ID	PN_05_03
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Generieren einer Signatur / AT
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, EXT

4.83.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.5

4.83.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_03-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_05_03-2	Sofern das Kommando GET CHALLENGE mit Secure Messaging ausgeführt werden soll: Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_05_03-3	Key Pair-Objekt mit dem Signaturschlüssel ist im Sicherheitsmodul vorhanden und ist aktiviert. (PN_04_09: Generierung eines ECC-Schlüsselpaares, PN_04_07: Aktivieren eines Key-Objektes)

4.83.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_03-4	Die Aufbereitung der zu signierenden Daten inkl. Hashen der Daten erfolgt

	durch das GW bzw. anderweitig außerhalb des Sicherheitsmoduls (Signaturdaten). Diese Signaturdaten bilden das zu signierende Token.
CN-PN_05_03-5	Als Signaturschlüssel wird ein Authentisierungsschlüssel (Schlüssel der Anwendungs-kategorie AT) verwendet.
CN-PN_05_03-6	Anwendung des Use Case im Rahmen der Erstellung eines Zertifikatsrequests zu einem ENC-Schlüssel. (UC_PN_04_12: Use Case „Erstellung eines Zertifikatsrequest-Pakets (SM-PKI)“)
CN-PN_05_03-7	Ausführung mit Secure Messaging.

4.83.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.83.6 Ablauf

Schritt	Beschreibung						
1	Aufbereitung des Tokens, d.h. der Signaturdaten inkl. Hashing (passend zur vorgesehenen Elliptischen Kurve / Schlüssellänge des Authentisierungsschlüssels).						
2	Bestimmung des Authentisierungsschlüssels bzw. des zugehörigen Key Pair-Objektes im Sicherheitsmodul (Speicherort im Filesystem, Key-ID). Selektion des DF, in dem der Authentisierungsschlüssel bzw. das zugehörige Key Pair-Objekt liegt. (PN_04_16: Selektieren eines DF/EF)						
3	MSE SET (AT): Interne Authentisierung (Übergabe der Key Reference des Key Pair-Objektes mit dem Authentisierungsschlüssel und Übergabe des zu verwendenden Krypto-Algorithmus)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	22	41	a4	LL	XX...XX	--
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus) '84-01-Key Reference' (für das Key Pair-Objekt)						
4	INTERNAL AUTHENTICATE (Token, d.h. Signaturdaten)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	88	00	00	LL	XX...XX	XX

	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält das Token als Oktett-String. 'Le' enthält die Anzahl der zu erwartenden Oktette.

4.83.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.84 Testfall: PN_05_04a

4.84.1 Informationen

ID	PN_05_04a
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Prüfen einer Signatur
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, EXT

4.84.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.5

4.84.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_04a-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_05_04a-2	Für das Kommando PSO VERIFY DIGITAL SIGNATURE in der Variante „ohne Übergabe des Public Key im Kommando“ (siehe

	untenstehende Variante 2) sowie für den Fall, dass das Kommando PSO VERIFY DIGITAL SIGNATURE in der Variante „mit Übergabe des Public Key im Kommando“ (siehe untenstehende Variante 1) mit Secure Messaging ausgeführt werden soll: Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)

4.84.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_04a-3	Die Aufbereitung der zu prüfenden Daten inkl. Hashen der Daten erfolgt durch das GW bzw. anderweitig außerhalb des Sicherheitsmoduls (Signaturprüfdaten).
CN-PN_05_04a-4	Die Ausführung des Kommandos PSO VERIFY DIGITAL SIGNATURE in der Variante „ohne Übergabe des Public Key im Kommando“ erfolgt stets mit Secure Messaging. Das Kommando PSO VERIFY DIGITAL SIGNATURE in der Variante „mit Übergabe des Public Key im Kommando“ kann mit oder ohne Secure Messaging ausgeführt werden; die das Kommando PSO VERIFY DIGITAL SIGNATURE aufrufende Stelle zeigt über das CLA-Byte im Kommando-Header an, ob das Kommando mit oder ohne Secure Messaging ausgeführt werden soll.

4.84.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.84.6 Ablauf

Schritt	Beschreibung						
1	Zusammenstellung der Signaturprüfdaten mit ihrer Signatur.						
2	Bestimmung des Signaturprüfchlüssels.						
3	PSO VERIFY DIGITAL SIGNATURE (Signaturprüfdaten, Signatur, Signaturprüfchlüssel)						
	CLA	INS	P1	P2	Lc	Data	Le

	00	2a	00	a8	LL	XX...XX	--
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '06-L06-OID 90-L90-Hash 9C-L9C-PubKey 9E-L9E-Signature' wobei OID = OID der Ellipt. Kurve, Hash = Oktett-String bel. Inhalts, aber passender Länge, PubKey = Public Key-Daten, Signature = 'R S' (Oktett-String, R und S von gleicher Oktett-Länge) Die Codierung der Public Key-Daten im Objekt '9C' erfolgt mit Uncompressed Encoding.						

4.84.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.85 Testfall: PN_05_04b

4.85.1 Informationen

ID	PN_05_04b
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Prüfen einer Signatur
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, EXT

4.85.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.5

4.85.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_04b-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_05_04b-2	Für das Kommando PSO VERIFY DIGITAL SIGNATURE in der Variante „ohne Übergabe des Public Key im Kommando“ (siehe untenstehende Variante 2) sowie für den Fall, dass das Kommando PSO VERIFY DIGITAL SIGNATURE in der Variante „mit Übergabe des Public Key im Kommando“ (siehe untenstehende Variante 1) mit Secure Messaging ausgeführt werden soll: Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_05_04b-3	Public Key-Objekt mit dem Signaturprüf Schlüssel ist im Sicherheitsmodul vorhanden und ist aktiviert. (PN_04_11: Import eines Public Key, PN_04_07: Aktivieren eines Key-Objektes)

4.85.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_04b-4	Die Aufbereitung der zu prüfenden Daten inkl. Hashen der Daten erfolgt durch das GW bzw. anderweitig außerhalb des Sicherheitsmoduls (Signaturprüfdaten).
CN-PN_05_04b-5	Die Ausführung des Kommandos PSO VERIFY DIGITAL SIGNATURE in der Variante „ohne Übergabe des Public Key im Kommando“ erfolgt stets mit Secure Messaging. Das Kommando PSO VERIFY DIGITAL SIGNATURE in der Variante „mit Übergabe des Public Key im Kommando“ kann mit oder ohne Secure Messaging ausgeführt werden; die das Kommando PSO VERIFY DIGITAL SIGNATURE aufrufende Stelle zeigt über das CLA-Byte im Kommando-Header an, ob das Kommando mit oder ohne Secure Messaging ausgeführt werden soll.

4.85.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.85.6 Ablauf

Schritt	Beschreibung

1	Zusammenstellung der Signaturprüfdaten mit ihrer Signatur.					
2	Bestimmung des Signaturprüfchlüssels bzw. des zugehörigen Public Key-Objektes im Sicherheitsmodul (Speicherort im Filesystem, Key-Name). Selektion des DF, in dem der Signaturprüfchlüssel bzw. das zugehörige Public Key-Objekt liegt. (PN_04_16: Selektieren eines DF/EF)					
3	MSE SET (DST): Signatur- und Zertifikatverifikation (Übergabe der Key Reference des Public Key-Objektes mit dem Signaturprüfchlüssel und Übergabe des zu verwendenden Krypto-Algorithmus)					
	CLA	INS	P1	P2	Lc	Data
	00	22	81	b6	LL	XX...XX
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Daten: '80-L80-CryptoID' (nur Wert, ohne Tag '06', für den Krypto-Algorithmus) '83-L83-Key Reference' (für das Public Key-Objekt)					
4	PSO VERIFY DIGITAL SIGNATURE (Signaturprüfdaten, Signatur)					
	CLA	INS	P1	P2	Lc	Data
	00	2a	00	a8	LL	XX...XX
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Daten: Signature Template gemäß [ISO 7816-8], Tab. 6: '90-L90-Hash 9E-L9E-Signature' wobei Hash = Oktett-String bel. Inhalts, aber passender Länge, Signature = 'R S' (Oktett-String, R und S von gleicher Oktett-Länge)					

4.85.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.86 Testfall: PN_05_05

4.86.1 Informationen

ID	PN_05_05

Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Aufbau eines TLS-Kanals zwischen externer Welt und SMGW / SMGW in der Rolle TLS-Client
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, EXT

4.86.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.5

4.86.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_05-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_05_05-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_05_05-3	TLS-Schlüsselpaar (GW_EXT_TLS_PRV, GW_EXT_TLS_PUB) des GW liegt im Sicherheitsmodul vor und ist aktiviert. (PN_04_07: Aktivieren eines Key-Objektes, PN_03_02: Wechsel der GW-System-PIN, PN_04_09: Generierung eines ECC-Schlüsselpaares)
CN-PN_05_05-4	TLS-Public Key GW_EXT_TLS_PUB des GW steht der externen Welt zur Verfügung. (VI_03_03: Export des Public Key eines vorläufigen GW-Schlüsselpaares (Vor-Personalisierung), PN_04_10: Export des Public Key eines ECC-Schlüsselpaares)
CN-PN_05_05-5	TLS-Schlüsselpaar (EXT_TLS_PRV, EXT_TLS_PUB) der externen Welt wurde durch diese generiert.
CN-PN_05_05-6	TLS-Public Key EXT_TLS_PUB der externen Welt liegt im GW vor.

4.86.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_05-7	Relevantes statisches TLS-Schlüsselmaterial: • TLS-Key Pair (GW_EXT_TLS_PRV, GW_EXT_TLS_PUB) des GW im Sicherheitsmodul • TLS-Key Pair (EXT_TLS_PRV, EXT_TLS_PUB) der externen Welt wobei EXT = Teilnehmer im WAN, LMN, HAN, ... Beim Wechsel der vorläufigen GW-Schlüsselpaare zu den GW-Betriebsschlüsselpaaren in der Teilphase „Personalisierung des SMGW“ bedeutet dies die Verwendung des vorläufigen TLS-Schlüsselpaars des GW und des TLS-Schlüsselpaars des GW-Administrators.
CN-PN_05_05-8	Relevantes ephemerales DH-Schlüsselmaterial: • DH-Key Pair (GW_PRV_EPH, GW_PUB_EPH) des GW im Sicherheitsmodul • DH-Key Pair (EXT_PRV_EPH, EXT_PUB_EPH) der externen Welt
CN-PN_05_05-9	Siehe auch die Beschreibungen zu ECKA-DH Protokoll-Variante 2.1 in [TR-03109-2], Kap. 4.5.5 a).
CN-PN_05_05-10	Ausführung mit Secure Messaging.

4.86.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_05-11	Ephemerales Schlüsselmaterial ist im Sicherheitsmodul nicht mehr vorhanden.

4.86.6 Ablauf

Schritt	Beschreibung
1	Zusammenstellung der Signaturprüfdaten mit ihrer Signatur.
2	PN_05_01: Erzeugen und Ausgeben einer Zufallszahl
3	PN_05_02: Generieren einer Signatur / DST
4	PN_05_04a: Prüfen einer Signatur
5	PN_04_11: Import eines Public Key
6	Ggf. Prüfung von Zertifikatsketten: Für TLS-Schlüssel im WAN, d.h. mit Zertifikaten aus der SM-PKI: Durchführung von (PN_04_13: Prüfung einer Zertifikatskette (SM-PKI))

7	"Ggf. Prüfung von Zertifikatsketten: Für TLS-Schlüssel außerhalb der SM-PKI: Prüfung einer Zertifikatskette auf analogem Weg unter Nutzung des Sicherheitsmoduls wie in (PN_04_13: Prüfung einer Zertifikatskette (SM-PKI))					
8	Externe Welt hat ephemerales DH-Key Pair (EXT_PRV_EPH, EXT_PUB_EPH) generiert und den Public Key EXT_PUB_EPH dem GW zugeliefert.					
9	MSE SET (AT): Schlüsselvereinbarung (Übergabe der Referenz auf die Protokoll-Variante 2.1)					
	CLA	INS	P1	P2	Lc	Data
	00	22	c1	a4	LL	XX...XX
'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') '83-L83-Key Reference' (für das Public Key-Objekt) '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)						
10	GENERAL AUTHENTICATE: ECKA-DH (Übergabe von EXT_PUB_EPH)					
	CLA	INS	P1	P2	Lc	Data
	00	86	00	00	LL	XX...XX
'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH						

	mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).

4.86.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.87 Testfall: PN_05_06

4.87.1 Informationen

ID	PN_05_06
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Aufbau eines TLS-Kanals zwischen externer Welt und SMGW / SMGW in der Rolle TLS-Server
Klassifizierung	Gutfall-Test
Phase	Normalbetrieb (End-Usage) des SMGW
Rollen	GW, EXT

4.87.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.5

4.87.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_06-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_05_06-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im

	Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_05_06-3	TLS-Schlüsselpaar (GW_EXT_TLS_PRV, GW_EXT_TLS_PUB) des GW liegt im Sicherheitsmodul vor und ist aktiviert. (PN_04_07: Aktivieren eines Key-Objektes, PN_04_09: Generierung eines ECC-Schlüsselpaares)
CN-PN_05_06-4	TLS-Public Key GW_EXT_TLS_PUB des GW steht der externen Welt zur Verfügung. (PN_04_10: Export des Public Key eines ECC-Schlüsselpaares)
CN-PN_05_06-5	TLS-Schlüsselpaar (EXT_TLS_PRV, EXT_TLS_PUB) der externen Welt wurde durch diese generiert.
CN-PN_05_06-6	TLS-Public Key EXT_TLS_PUB der externen Welt liegt im GW vor.
CN-PN_05_06-7	Temporäres Key Pair-Objekt Key.EPH_x für das ephemere Schlüsselmaterial des GW ist im Sicherheitsmodul angelegt.

4.87.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_06-8	Relevantes statisches TLS-Schlüsselmaterial: • TLS-Key Pair (GW_EXT_TLS_PRV, GW_EXT_TLS_PUB) des GW im Sicherheitsmodul • TLS-Key Pair (EXT_TLS_PRV, EXT_TLS_PUB) der externen Welt wobei EXT = Teilnehmer im LMN oder HAN.
CN-PN_05_06-9	Relevantes ephemerales DH-Schlüsselmaterial: • DH-Key Pair (GW_PRV_EPH, GW_PUB_EPH) des GW im Sicherheitsmodul • DH-Key Pair (EXT_PRV_EPH, EXT_PUB_EPH) der externen Welt
CN-PN_05_06-10	Siehe auch die Beschreibungen zu ECKA-DH Protokoll-Variante 2.2 in [TR-03109-2], Kap. 4.5.5 a). Die temporäre Speicherung des DH-Key Pair (GW_PRV_EPH, GW_PUB_EPH) des GW erfolgt im Sicherheitsmodul im Key Pair-Objekt Key.EPH_x im MF.
CN-PN_05_06-11	Ausführung mit Secure Messaging.

4.87.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_06-12	Ephemerales Schlüsselmaterial ist im Sicherheitsmodul nicht mehr

	vorhanden.

4.87.6 Ablauf

Schritt	Beschreibung														
1	PN_05_01: Erzeugen und Ausgeben einer Zufallszahl														
2	PN_05_02: Generieren einer Signatur / DST														
3	PN_05_04a: Prüfen einer Signatur														
4	PN_04_11: Import eines Public Key														
5	Ggf. Prüfung von Zertifikatsketten: Prüfung einer Zertifikatskette auf analogem Weg unter Nutzung des Sicherheitsmoduls wie in (PN_04_13: Prüfung einer Zertifikatskette (SM-PKI))														
6	Selektion des DF, in dem das Key Pair-Objekt Key.EPH_x für das ephemere Schlüsselmateriale des GW liegt. (PN_04_16: Selektieren eines DF/EF)														
7	GENERATE ASYMMETRIC KEY PAIR: Schlüsselgenerierung mit Ausgabe des Public Key (Übergabe der Key Reference des Key Pair-Objektes Key.EPH_x sowie der OID für die vorgesehene Elliptische Kurve für die Generierung des ephemeralen Schlüsselmateriale des GW mit Ablage im Key Pair-Objekt Key.EPH_x und Ausgabe des ephemeralen Public Key an das GW)														
	<table><tr><th>CLA</th><th>INS</th><th>P1</th><th>P2</th><th>Lc</th><th>Data</th><th>Le</th></tr><tr><td>00</td><td>47</td><td>82</td><td>00</td><td>LL</td><td>XX...XX</td><td>XX</td></tr></table>	CLA	INS	P1	P2	Lc	Data	Le	00	47	82	00	LL	XX...XX	XX
	CLA	INS	P1	P2	Lc	Data	Le								
	00	47	82	00	LL	XX...XX	XX								
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette.														
'Data' enthält die Daten: a) Für ein Key-Paar, das für Signaturzwecke verwendet werden soll (Anwendungsklasse DST): 'B6-LB6-(84-01-Key Reference) 7F49-L7F49-KeyParameter' b) Für ein Key-Paar, das für Zwecke der Authentisierung verwendet werden soll (Anwendungsklasse AT): 'A4-LA4-(84-01-Key Reference) 7F49-L7F49-KeyParameter' Das CRT-Template (DST-Template bzw. AT-Template) enthält die Referenz auf das Key Pair-Objekt (Tag '84'), in dem das zu generierende Key-Paar gespeichert werden soll. KeyParameter = '06-L06-OID der Ellipt. Kurve' Für temporäre Key Pair-Objekte wird nur das AT-Template benötigt.															
'Le' enthält die Anzahl der zu erwartenden Oktette.															
8	Aufbereitung der Server Key Exchange Message durch das GW.														
9	Zur Signatur der Server Key Exchange Message des GW unter Nutzung des Schlüssels GW_EXT_TLS_PRV Durchführung von (PN_05_02: Generieren einer Signatur / DST)														

10	Externe Welt generiert ephemerales DH-Key Pair (EXT_PRV_EPH, EXT_PUB_EPH) und liefert den Public Key EXT_PUB_EPH dem GW zu.						
11	MSE SET (AT): Schlüsselvereinbarung (Übergabe der Referenz auf die Protokoll-Variante 2.2 und Übergabe der Key Reference (mit Anzeige globaler Suche) des Key Pair-Objektes Key.EPH_x)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	22	c1	a4	LL	XX...XX	--
'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') '83-L83-Key Reference' (für das Public Key-Objekt) '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)							
12	GENERAL AUTHENTICATE: ECKA-DH (Übergabe von EXT_PUB_EPH)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	86	00	00	LL	XX...XX	XX
'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) 'A0-LA0- 06-L06-OIDCurve (OID der ElliptischenKurve) 86-L86-EphPubKey' (hier: EXT_PUB_EPH) b) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt).							

4.87.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.88 Testfall: PN_05_07

4.88.1 Informationen

ID	PN_05_07
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Inhaltsdatenverschlüsselung mit SMGW/Sicherheitsmodul als Recipient
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, EXT

4.88.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.5

4.88.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_07-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_05_07-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_05_07-3	Statisches ENC-Key Pair (GW_PRV_STAT, GW_PUB_STAT) des GW liegt im Sicherheitsmodul vor und ist aktiviert. (PN_04_07: Aktivieren eines Key-Objektes, PN_04_09: Generierung eines ECC-Schlüsselpaars)

CN-PN_05_07-4	Der externen Welt (EXT = Teilnehmer im WAN, LMN, HAN, ...) steht GW_PUB_STAT zur Verfügung. (PN_04_10: Export des Public Key eines ECC-Schlüsselpaares)
CN-PN_05_07-5	Ephemerales ENC-Key Pair (EXT_PRV_EPH, EXT_PUB_EPH) der externen Welt wurde durch diese generiert.
CN-PN_05_07-6	Ephemeraler ENC-Public Key EXT_PUB_EPH der externen Welt liegt im GW vor.

4.88.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_07-7	Relevantes statisches ENC-Schlüsselmaterial: • ENC-Key Pair (GW_PRV_STAT, GW_PUB_STAT) des GW im Sicherheitsmodul Relevantes ephemerales ENC-Schlüsselmaterial: • ENC-Key Pair (EXT_PRV_EPH, EXT_PUB_EPH) der externen Welt
CN-PN_05_07-8	Siehe auch die Beschreibungen zu ECKA-EG Protokoll-Variante 1.1 in [TR-03109-2], Kap. 4.5.5 a).
CN-PN_05_07-9	Ausführung mit Secure Messaging.

4.88.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_07-10	Ephemerales Schlüsselmaterial ist im Sicherheitsmodul nicht mehr vorhanden.

4.88.6 Ablauf

Schritt	Beschreibung						
1	MSE SET (AT): Schlüsselvereinbarung (Übergabe der Referenz auf die Protokoll-Variante 1.1 und Übergabe der Key Reference des Key Pair-Objektes für GW_PRV_STAT)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	22	c1	a4	LL	XX...XX	--

	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') '83-L83-Key Reference' (für das Public Key-Objekt) '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)					
2	GENERAL AUTHENTICATE: ECKA-DH (Übergabe von EXT_PUB_EPH)					
	CLA	INS	P1	P2	Lc	Data
	00	86	00	00	LL	XX...XX
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).					

4.88.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.89 Testfall: PN_05_08a

4.89.1 Informationen

ID	PN_05_08a
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Inhaltsdatenverschlüsselung mit SMGW/Sicherheitsmodul als Initiator
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, EXT

4.89.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.5

4.89.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_08a-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_05_08a-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_05_08a-3	Statisches ENC-Key Pair (EXT_PRV_STAT, EXT_PUB_STAT) der externen Welt wurde durch diese generiert. (EXT = Teilnehmer im WAN, LMN, HAN, ...)
CN-PN_05_08a-4	Statischer ENC-Public Key EXT_PUB_STAT steht dem GW zur Verfügung.

4.89.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung

CN-PN_05_08a-5	Relevantes ephemerales ENC-Schlüsselmaterial: • ENC-Key Pair (GW_PRV_EPH, GW_PUB_EPH) des GW im Sicherheitsmodul Relevantes statisches ENC-Schlüsselmaterial: • ENC-Key Pair (EXT_PRV_STAT, EXT_PUB_STAT) der externen Welt
CN-PN_05_08a-6	Siehe auch die Beschreibungen zu ECKA-EG Protokoll-Variante 1.2 in [TR-03109-2], Kap. 4.5.5 a).
CN-PN_05_08a-7	Ausführung mit Secure Messaging.

4.89.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.89.6 Ablauf

Schritt	Beschreibung						
1	Sofern der Schlüssel nicht schon im Sicherheitsmodul vorliegt, Import von EXT_PUB_STAT (PN_04_11: Import eines Public Key)						
2	MSE SET (AT): Schlüsselvereinbarung (Übergabe der Referenz auf die Protokoll-Variante 1.2 und Übergabe der Key Reference des Public Key-Objektes für EXT_PUB_STAT)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	22	c1	a4	LL	XX...XX	--
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') '83-L83-Key Reference' (für das Public Key-Objekt) '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-						

	Server) '80-L80-OID Key Agreement-Protokoll' '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)						
3	GENERAL AUTHENTICATE: ECKA-DH (Übergabe von EXT_PUB_STAT)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	86	00	00	LL	XX...XX	XX
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).						
4	Übermittlung von GW_PUB_EPH (ausgegeben von GENERAL AUTHENTICATE) an die externe Welt.						

4.89.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.90 Testfall: PN_05_08b

4.90.1 Informationen

ID	PN_05_08b
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Inhaltsdatenverschlüsselung mit SMGW/Sicherheitsmodul als Initiator
Klassifizierung	Gutfall-Test

Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, EXT

4.90.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.5

4.90.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_08b-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_05_08b-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_05_08b-3	Statisches ENC-Key Pair (EXT_PRV_STAT, EXT_PUB_STAT) der externen Welt wurde durch diese generiert. (EXT = Teilnehmer im WAN, LMN, HAN, ...)
CN-PN_05_08b-4	Statischer ENC-Public Key EXT_PUB_STAT steht dem GW zur Verfügung.

4.90.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_08b-5	Relevantes ephemerales ENC-Schlüsselmaterial: • ENC-Key Pair (GW_PRV_EPH, GW_PUB_EPH) des GW im Sicherheitsmodul Relevantes statisches ENC-Schlüsselmaterial: • ENC-Key Pair (EXT_PRV_STAT, EXT_PUB_STAT) der externen Welt
CN-PN_05_08b-6	Siehe auch die Beschreibungen zu ECKA-EG Protokoll-Variante 1.2 in [TR-03109-2], Kap. 4.5.5 a).
CN-PN_05_08b-7	Ausführung mit Secure Messaging.

4.90.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.90.6 Ablauf

Schritt	Beschreibung						
1	MSE SET (AT): Schlüsselvereinbarung (Übergabe der Referenz auf die Protokoll-Variante 1.2)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	22	c1	a4	LL	XX...XX	--
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Daten: '80-L80-OID Key Agreement-Protokoll' (nur Wert ohne Tag '06') '83-L83-Key Reference' (für das Public Key-Objekt) '84-01-Key Reference' (für das Key Pair-Objekt) (je nach Protokoll-Variante fehlen evtl. DOs) Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a) Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient '80-L80-OID Key Agreement-Protokoll' '84-01-Key Reference' (hier: Key Reference von GW_PRV_STAT) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/Sicherheitsmodul als Initiator bei Übergabe von EXT_PUB_STAT im Kommando GENERAL AUTHENTICATE: '80-L80-OID Key Agreement-Protokoll' wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: '80-L80-OID Key Agreement-Protokoll' '83-L83-Key Reference' (hier: Key Reference von EXT_PUB_STAT) c) Protokoll-Variante 2.1: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Client) '80-L80-OID Key Agreement-Protokoll' d) Protokoll-Variante 2.2: ECKA-DH mit SMGW/Sicherheitsmodul als Initiator oder Recipient (TLS-Server) '80-L80-OID Key Agreement-Protokoll' '84-01-Key Reference' (hier: Key Reference von GW_PRV_EPH)						
2	GENERAL AUTHENTICATE: ECKA-DH (Übergabe von EXT_PUB_STAT)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	86	00	00	LL	XX...XX	XX
	'Lc' enthält die Anzahl der in den Kommandodaten enthaltenen Oktette. 'Data' enthält die Daten: '7C-L7C-Protokoll-spezifische Datenobjekte', genauer: 'A0-LA0- 06-L06-OIDCurve (OID der ElliptischenKurve) 86-L86-PublicKey' (Public Key-Daten) (je nach Protokoll-Variante fehlen evtl. DOs) Die Codierung der Public Key-Daten im Objekt '86' erfolgt jeweils mit Uncompressed Encoding. Für die verschiedenen ECKA-Protokoll-Varianten sieht dies im Detail wie folgt aus: a)						

	Protokoll-Variante 1.1: ECKA-EG mit SMGW/Sicherheitsmodul als Recipient 'A0-LA0- 86-L86-EphPubKey' (hier: EXT_PUB_EPH) (hier: OID der Elliptischen Kurve implizit bekannt) b) Protokoll-Variante 1.2: ECKA-EG mit SMGW/ Sicherheitsmodul als Initiator sofern Key-Übergabe im Kommando: 'A0-LA0- 06-L06-OIDCurve (OID der ElliptischenKurve) 86-L86-StatPubKey' (hier: EXT_PUB_STAT) wenn EXT_PUB_STAT schon im Sicherheitsmodul vorliegt: --- (leeres '7C'-Template).
3	Übermittlung von GW_PUB_EPH (ausgegeben von GENERAL AUTHENTICATE) an die externe Welt.

4.90.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.91 Testfall: PN_05_09

4.91.1 Informationen

ID	PN_05_09
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Inhaltsdatensignatur / Signaturgenerierung
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, EXT

4.91.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.5

4.91.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_09-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_05_09-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_05_09-3	SIG-Key Pair (GW_WAN_SIG_PRV, GW_WAN_SIG_PUB) des GW liegt im Sicherheitsmodul vor und ist aktiviert. (PN_04_09: Generierung eines ECC-Schlüsselpaares)
CN-PN_05_09-4	Ggf. auch (PN_04_07: Aktivieren eines Key-Objektes)
CN-PN_05_09-5	Signaturdaten (Inhaltsdaten in geeignet aufbereiteter Form) liegen im GW vor.

4.91.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_09-6	Die Aufbereitung der zu signierenden Inhaltsdaten inkl. Hashen der Daten erfolgt durch das GW bzw. anderweitig außerhalb des Sicherheitsmoduls (Signaturdaten).
CN-PN_05_09-7	Relevantes Signaturschlüsselmaterial: • SIG-Key Pair (GW_WAN_SIG_PRV, GW_WAN_SIG_PUB) des GW im Sicherheitsmodul
CN-PN_05_09-8	Ausführung mit Secure Messaging.

4.91.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.91.6 Ablauf

Schritt	Beschreibung
1	Mit GW_WAN_SIG_PRV als Signaturschlüssel zur Signatur der Signaturdaten Durchführung von (PN_05_02: Generieren einer Signatur / DST)

4.91.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.92 Testfall: PN_05_10

4.92.1 Informationen

ID	PN_05_10
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Inhaltsdatensignatur / Signaturprüfung
Klassifizierung	Gutfall-Test
Phase	Installation + Vor-Ort-Inbetriebnahme des SMGW, Normalbetrieb (End-Usage) des SMGW
Rollen	GW, EXT

4.92.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.5

4.92.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_10-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_05_10-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)
CN-PN_05_10-3	SIG-Key Pair (EXT_SIG_PRV, EXT_SIG_PUB) der externen Welt wurde durch diese generiert. (EXT = Teilnehmer im WAN, LMN, HAN, ...)

CN-PN_05_10-4	EXT_SIG_PUB steht dem GW zur Verfügung.
CN-PN_05_10-5	Signaturprüfdaten (Inhaltsdaten in geeignet aufbereiteter Form) mit zu prüfender Signatur liegen im GW vor.

4.92.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_10-6	Die Aufbereitung der zu prüfenden Inhaltsdaten inkl. Hashen der Daten erfolgt durch das GW bzw. anderweitig außerhalb des Sicherheitsmoduls (Signaturprüfdaten). Relevantes Signaturschlüsselmaterial: • SIG-Key Pair (EXT_SIG_PRV, EXT_SIG_PUB) der externen Welt
CN-PN_05_10-7	Ausführung mit Secure Messaging.

4.92.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.92.6 Ablauf

Schritt	Beschreibung
1	Für den Import von EXT_SIG_PUB, sofern der Signaturprüf Schlüssel EXT_SIG_PUB noch nicht im Sicherheitsmodul vorliegt, Durchführung von (PN_04_11: Import eines Public Key)
2	Mit EXT_SIG_PUB als Signaturprüf Schlüssel zur Prüfung der Signatur über die Signaturprüfdaten Durchführung von (PN_05_04: Prüfen einer Signatur)

4.92.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

4.93 Testfall: PN_05_11

4.93.1 Informationen

ID	PN_05_11
Beschreibung	Dieser Test ist ein Usecase-Szenario mit dem Inhalt: Generieren eines TLS-Schlüsselpaars für einen Zähler
Klassifizierung	Gutfall-Test
Phase	Normalbetrieb (End-Usage) des SMGW
Rollen	GW, EXT

4.93.2 Referenzen

Der Testfall bezieht sich auf das Dokument: BSI TR-03109-2, Anhang: Smart Meter Gateway – Sicherheitsmodul – Use Cases, Version 1.1, Kapitel 4.5

4.93.3 Vorbedingungen

Folgende Bedingungen müssen vor Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_11-1	Sicherheitsmodul befindet sich nicht im Zustand "terminiert"
CN-PN_05_11-2	Erfolgreiche Ausführung des PACE-Protokolls zwischen GW und Sicherheitsmodul, d.h. der Sicherheitszustand PACE ist im Sicherheitsmodul gesetzt. (PN_03_01: PACE-Authentisierung)

4.93.4 Nebenbedingung

Folgende Bedingungen müssen während Ausführung des Testfalls erfüllt sein:

ID	Beschreibung
CN-PN_05_11-3	Da für im Sicherheitsmodul generierte Schlüsselpaare ein Export des kompletten Schlüsselpaars (genauer ein Export des privaten Schlüsselteils) nicht möglich ist, wird das Sicherheitsmodul für die Schlüsselgenerierung von TLS-Schlüsselpaaren der Zähler auf folgende Weise eingebunden. Das Sicherheitsmodul liefert über seine Zufallszahlengenerierung eine hochwertige Zufallszahl, die das GW als

	privaten ECC-Schlüssel interpretiert und weiterverwendet. Das GW übernimmt die Aufgabe der Berechnung des zugehörigen öffentlichen ECC-Schlüssels aus dem privaten Schlüssel (d.h. aus der vom Sicherheitsmodul gelieferten Zufallszahl).
CN-PN_05_11-4	Ausführung mit Secure Messaging.

4.93.5 Nachbedingungen

Folgende Bedingungen müssen nach Ausführung des Testfalls erfüllt sein:

n/a

4.93.6 Ablauf

Schritt	Beschreibung						
1	Bestimmung der Elliptischen Kurve, zu der das Schlüsselpaar generiert werden soll.						
2	GET CHALLENGE (Anzeige der gewünschten Länge der Zufallszahl im Kommando)						
	CLA	INS	P1	P2	Lc	Data	Le
	00	84	XX	00	--	--	XX
	'P1' enthält '00': generierte Zufallszahl wird intern gespeichert '01': generierte Zufallszahl wird intern nicht gespeichert. 'Le' enthält die Anzahl der Oktette zu erwartenden Zufallszahl (Hersteller-abhängig und in Abhängigkeit vom Ausgabeformat).						

4.93.7 Erwartete Ergebnisse

ID	Beschreibung
RS-232B	Die Durchführung aller Testschritte erfolgt ohne Fehler bzgl. der Return-Codes von Kommando-Nachrichten und informellen Beschreibungen des Testfalls.

Literaturverzeichnis

- BSI TR-03109-1: Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, Version 1.0, 2013, Bundesamt für Sicherheit in der Informationstechnik
- BSI TR-03109-2: Smart Meter Gateway – Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls, Version 1.1, 2014, Bundesamt für Sicherheit in der Informationstechnik
- PP-0077: Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP), Version 1.03, 2014, Bundesamt für Sicherheit in der Informationstechnik
- BSI TR-03109-TS-2: Testspezifikation zur Prüfung des Sicherheitsmoduls nach BSI TR-03109-2, V1.0, 2018, Bundesamt für Sicherheit in der Informationstechnik
- BSI TR-03109-TS-2-Testkonzept: Testkonzept für das Sicherheitsmodul nach BSI TR-03109-2, V1.0, 2018, Bundesamt für Sicherheit in der Informationstechnik
- BSI TR-03109-TS-2-Testidentifikation: Identifikation relevanter Testfälle für das Sicherheitsmodul nach BSI TR-03109-2, V1.0, 2018, Bundesamt für Sicherheit in der Informationstechnik
- BSI TR-03109-TS-2-XML: BSI-TR-03109-TS-2-XML_SM_V1.0.zip, Version 1.0, 2018, Bundesamt für Sicherheit in der Informationstechnik