Bundesamt
für Sicherheit in der
Informationstechnik

Technische Richtlinie BSI TR-03116 Kryptographische Vorgaben für Projekte der Bundesregierung

Teil 2: Hoheitliche Dokumente

Stand 2018

Datum: 23. April 2018

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

E-Mail: eid@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Tabellenverzeichnis

1 Einleitung

Die Technische Richtlinie BSI TR-03116 stellt eine Vorgabe für Projekte des Bundes dar. Die Technische Richtlinie ist in vier Teile gegliedert:

- Teil 1 der Technischen Richtlinie beschreibt die Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren im Gesundheitswesen für die elektronische Gesundheitskarte (eGK), den Heilberufeausweis (HBA) und der technischen Komponenten der Telematikinfrastruktur.
- Der vorliegende Teil 2 der Technischen Richtlinie beschreibt die Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren in hoheitlichen Ausweisdokumenten, zur Zeit für den elektronischen Reisepass, den elektronischen Personalausweis, den elektronischen Aufenthaltstitel und den Ankunftsnachweis.
- Teil 3 der Technischen Richtlinie beschreibt die Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren in der Infrastruktur intelligenter Messsysteme im Energiesektor.
- Teil 4 der Technischen Richtlinie beschreibt die Sicherheitsanforderungen für den Einsatz der Kommunikationsverfahren SSL/TLS, S/MIME, SAML und OpenPGP in Anwendungen des Bundes.

Die Vorgaben des vorliegenden Teil 2 der Technischen Richtlinie basieren auf Prognosen über die Sicherheit der in hoheitlichen Dokumenten verwendeten kryptographischen Verfahren. Aufgrund der langen Gültigkeitszeit von hoheitlichen Dokumente erfolgt die Prognose für die Verwendung in der Ausgabe von Dokumenten über einen Zeitraum von 4 Jahren, zur Zeit bis einschließlich 2021. Eine weitere Verwendung des Verfahrens über diesen Zeitraum hinaus ist nicht ausgeschlossen und wird mit 2021+ gekennzeichnet.

Unabhängig davon besteht die Möglichkeit den elektronischen Teil bereits ausgegebene hoheitliche Dokumente durch Rückruf des verwendeten Document Signer Zertifikates (vgl. Abschnitt 2.1) zu sperren. Das physikalische Ausweisdokument behält jedoch auch in diesem Fall seine Gültigkeit.

1.1 Hoheitliche Ausweisdokumente

Die Technische Richtlinie legt verbindlich die Vorgaben für den Einsatz von kryptographischen Verfahren basierend auf der TR-02102-1 [1] für folgende hoheitliche Ausweisdokumente fest:

- Elektronischer Reisepass
- Elektronischer Personalausweis
- Elektronischer Aufenthaltstitel
- Ankunftsnachweis

Abweichungen von den Empfehlungen aus TR-02102-1 werden in den einzelnen Abschnitten erläutert.

Darüber hinaus enthält diese Technische Richtlinie Empfehlungen für Terminals, welche von den verbindlichen Vorgaben für hoheitliche Dokumente abweichen können.

Standard	*Kryptographisches Verfahren*
ICAO Doc 9303	Basic Access Control
	Passive Authentisierung
	Aktive Authentisierung
ICAO TR-PACE	Password Authenticated Connection Establishment
BSI TR-03110, Parts 1-3	Extended Access Control Version 1 & 2
	– Chip Authentisierung 1 & 2
	– Terminal Authentisierung 1 & 2
	Password Authenticated Connection Establishment
	Restricted Identification
BSI TR-03137	Digital Seal

Tabelle 1: Kryptographische Verfahren

1.2 eIDAS-Verordnung

Die eIDAS-Verordnung [2] regelt die Rahmenbedingungen für die gegenseitige Anerkennung von elektronischen Identifizierungsmitteln im Europäischen Wirtschaftsraum. Hierbei können Mitgliedsstaaten ihre nationalen Systeme zur Identifizierung von natürlichen oder juristischen Personen bei der Kommission *notifizieren*.

Die Anerkennung von notifizierten elektronischen Identifizierungsmitteln durch öffentliche Stellen wird entsprechend der Regelungen dieser Verordnung [2] zum 28.09.2018 verpflichtend. Die Interoperabilität wird über ein sogenanntes *Interoperability Framework* [3] realisiert.

1.3 Kryptographische Verfahren und Standards

Hoheitliche Ausweisdokumente sind durch eine Reihe von internationalen, europäischen und nationalen Standards festgelegt. Tabelle 1 gibt einen Überblick über die kryptographischen Verfahren.

1.3.1 Internationale Reisedokumente

Der elektronische Reisepass und der elektronische Aufenthaltstitel (nach Vorgaben der EU-Kommission) sind internationale Reisedokumente.

Der internationale Standard für Reisedokumente wird von der ICAO in Doc 9303 [4][1] festgelegt. Die von der ICAO standardisierten kryptographischen Verfahren sind:

– Password Authenticated Connection Establishment,

1 Das Verfahren Password Authenticated Connection Establishment (PACE) gemäß ICAO Doc 9303 [4] ist kompatibel zur Technischen Richtlinie BSI TR-03110 [5] und stammt ursprünglich aus einer älteren Version der BSI TR-03110.

- Basic Access Control,
- Passive Authentisierung und
- Aktive Authentisierung.

1.3.2 Europäische Reisedokumente

Der elektronische Reisepass und der elektronische Aufenthaltstitel (nach Vorgaben der EU-Kommission) sind europäische Reisedokumente.

Die EU hat über die Verordnung (EC) No 2252/2004 [6] die Kommission mit der Standardisierung von zusätzlichen Verfahren zur Integration von Fingerabdrücken in Reisedokumenten beauftragt. Die Technischen Spezifikationen sind in den Kommissionsentscheidungen C(2006) 2909 [7], C(2011) 5478 [8], C(2011) 5499 [9], C(2013) 6178 [10] und C(2013) 6181 [11] dargelegt und verweisen auf die Technische Richtlinie BSI TR-03110 und den ICAO Technical Report [12], der von der ICAO mittlerweile in ICAO Doc 9303 integriert wurde.

Folgende der in der Technische Richtlinie BSI TR-03110, Part 1 [5] spezifizierten kryptographischen Verfahren sind für europäische Reisedokumente relevant:

- Extended Access Control Version 1, d.h.
  - Chip Authentisierung Version 1[2]
  - Terminal Authentisierung Version 1

Folgendes der im ICAO Doc 9303 [4] spezifizierten kryptographischen Verfahren ist für europäische Reisedokumente relevant:

- Passive Authentisierung
- Password Authenticated Connection Establishment (kompatibel zu [5])

1.3.3 Nationale Ausweisdokumente

Nationale Ausweisdokumente sind nicht notwendigerweise konform zu den Spezifikationen für Reisedokumente. Der elektronische Personalausweis und der elektronische Aufenthaltstitel sind nationale Ausweisdokumente.

Folgende der in der Technische Richtlinie BSI TR-03110, Part 2 [13] spezifizierten kryptographischen Verfahren sind für nationale Ausweisdokumente relevant:

- Extended Access Control Version 2, d.h.
  - Chip Authentisierung Version 2
  - Terminal Authentisierung Version 2
- Passive Authentisierung
- Password Authenticated Connection Establishment
- Restricted Identification.

2 Das Verfahren wurde von der ICAO mittlerweile auch in die Doc 9303 [4] aufgenommen.

1.4 Kryptographische Algorithmen

1.4.1 Basisverfahren

Tabelle 2 gibt einen Überblick über die in hoheitlichen Dokumenten verwendeten kryptographischen Basisverfahren. Das Verfahren 2-Key-3DES wird in der Technischen Richtlinie TR-02102 [1] nicht mehr empfohlen. Die Aufnahme dieses Verfahrens in dieser Technischen Richtlinie gilt nur für den elektronischen Reisepass und den elektronischen Aufenthaltstitel aufgrund der internationalen bzw. europäischen Standardisierung.

Verfahren	***Algorithmus***
Digitale Signatur	ECDSA [14]
Schlüsseleinigung	ECKA [14]
Blockchiffre Verschlüsselungsmodi MAC-Modi	AES [15] - CBC-Mode [16] - CMAC Mode [17]
Blockchiffre Verschlüsselungsmodi MAC-Modi	2-Key-3DES[3] [18] - CBC-Mode [16] - Retail MAC[4] [19]
Hash	SHA-1 (bis 2010) und SHA-2 [20]

Tabelle 2: Kryptographische Algorithmen

1.4.2 Domainparameter für Elliptische Kurven

Für kryptographische Algorithmen basierend auf Elliptischen Kurven (d.h. ECDSA und ECKA) sind die Brainpool Domain Parameter [21] in den entsprechenden Bitlängen zu verwenden.

1.4.3 Zufallszahlengeneratoren

Für die Erzeugung von Zufallszahlen und kryptographischen Schlüsseln (inkl. ephemeralen Schlüsseln) sind in allen verwendeten kryptographischen Protokollen Zufallszahlengeneratoren aus einer der folgenden Klassen (siehe [22]) zu verwenden:

- DRG.4
- PTG.2 oder höher.

Bei der Verwendung von PTG.2 muss ggf. eine anwendungsspezifische kryptographische Nachbearbeitung der Zufallszahlen erfolgen, um eine mögliche Schiefe der Zufallszahlen zu verhindern. Es wird empfohlen, einen Zufallszahlengenerator der Klasse PTG.3 zu verwenden.

3 In [18] auch mit TDEA Keying Option 2 bezeichnet.
4 Gemäß [19] auch als MAC Algorithmus 3 mit DEA bezeichnet.

1.4.3.1 PTG.2 - Nachbearbeitung bei PACE

Bei PACE wird eine 128 Bit Zufallszahl s erzeugt und anschließend zu $z=E_K(s)$ verschlüsselt. Wird hierbei ein Zufallszahlengenerator der Klasse PTG.2 verwendet, so muss die Erzeugung von s unter Einbeziehung einer zur Klasse DRG.3 konformen kryptographischen Nachbearbeitung erfolgen.

Alternativ kann folgende Variante des PACE-Algorithmus verwendet werden:

- Es werden zwei 128 Bit Zufallszahlen s_1 und s_2 mit einem Zufallszahlengenerator der Klasse PTG.2 erzeugt.
- Anschließend wird der Chiffretext $(c||s||z) = E_K(s_1||s_2||0)$ wie in Abbildung 1 dargestellt berechnet.
- Der Wert c wird verworfen, die Werte s und z ($=E_K(s)$) werden wie bisher verwendet.

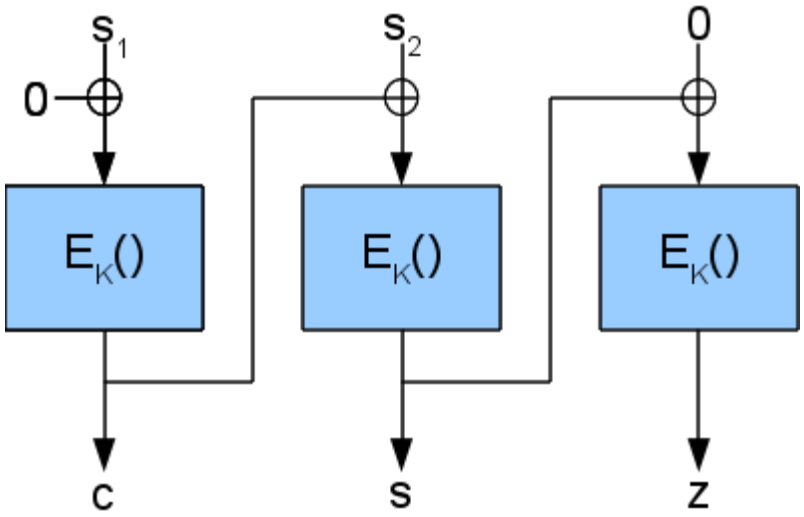

Abbildung 1: Alternative Verschlüsselung der PACE Nonce

Sofern eine andere Nachbearbeitung verwendet wird, muss diese mit dem BSI abgestimmt werden.

2 Public Key Infrastrukturen

Es werden zwei unterschiedliche Arten von Public Key Infrastrukturen verwendet:

- Eine Public Key Infrastruktur (*Dokumenten-PKI*) zur Überprüfung der Authentizität hoheitlicher Dokumente bzw. der darauf enthaltenen, relevanten Daten (Passive Authentisierung bzw. Digitales Siegel).
- Mehrere anwendungsspezifische Public Key Infrastrukturen (Berechtigungs-PKIen) zur Festlegung von Berechtigungen von Lesegeräten (Terminal Authentisierung).

Darüber hinaus werden für die grenzüberschreitende Verwendung von Online-Diensten im Kontext der eIDAS-Verordnung [2] so genannte *eIDAS-Knoten* (*eIDAS-Konnektoren* und *eIDAS-Services*) (vgl. [3], [23]) eingesetzt.

Hierfür werden innerhalb der Berechtigungs-PKI für die eID-Anwendung *Metadaten-Signer-Zertifikate* (*MDS-Zertifikate*) ausgegeben, welche zur grenzüberschreitenden Überprüfung der Authentizität der Metadaten von Online-Diensten in Deutschland durch eIDAS-Services anderer Mitgliedsstaaten dienen.

2.1 Dokumenten-PKI

Die Authentizität des elektronischen Teils hoheitlicher Dokumente kann durch die Passive Authentisierung (in Verbindung mit der Chip Authentisierung) geprüft werden. Ankunftsnachweise enthalten anstelle eines Chips ein digitales Siegel als zusätzliches Sicherheitsmerkmal, mit dem Identitätsdaten des Nachweisinhabers authentifiziert werden.

Die Passive Authentisierung und die digitalen Siegel basieren auf der Dokumenten-PKI bestehend aus einer *Country Signing Certification Authority* als nationale Wurzelinstanz und für jeden autorisierten Herausgeber des hoheitlichen Dokuments mindestens einem *Document Signer*.

2.1.1 CSCA

Das Signaturverfahren, mit dem die X.509-Zertifikate signiert werden, wird durch die Country Signing Certification Authority festgelegt. Die Country Signing Certification Authority wird vom BSI betrieben.

Tabelle 3 legt die von der CSCA für die Ausstellung von Zertifikaten zu verwendenden kryptographischen Verfahren verbindlich fest. Die Verwendungszeiträume beziehen sich auf die Dokumentenproduktion.

Verfahren	***Algorithmus***	***Länge***	***Verwendung von***	***Verwendung bis***
Country Signing CA				
Signatur	ECDSA	256 384 512	 2011 2019	2011 2019 2021+
Hash	SHA-256 SHA-384 SHA-512	256 384 512	 2011 2019	2011 2019 2021+

Tabelle 3: CSCA

2.1.2 Passive Authentisierung

Tabelle 4 legt die für die Passive Authentisierung zu verwendenden kryptographischen Verfahren verbindlich fest. Die Verwendungszeiträume beziehen sich auf die Dokumentenproduktion.

Verfahren	*Algorithmus*	*Länge*	*Verwendung von*	*Verwendung bis*
Document Signer				
Signatur	ECDSA	224 256 384	 2010 2019[5]	2010 2019 2021+
Hash	SHA-224 SHA-256 SHA-384	224 256 384	 2010 2019[5]	2010 2019 2021+
Passive Authentisierung				
Hash von Datengruppen	SHA-1 SHA-256 SHA-384	160 256 384	 2010 2019[5]	2010 2019 2021+

Tabelle 4: Passive Authentisierung

2.1.3 Digitale Siegel

Tabelle 5 legt die für digitale Siegel zu verwendenden kryptographischen Verfahren verbindlich fest. Die Verwendungszeiträume beziehen sich auf die Siegelerstellung.

Verfahren	*Algorithmus*	*Länge*	*Verwendung von*	*Verwendung bis*
Barcode Signer				
Signatur	ECDSA	256	2016	2021+
Hash	SHA-256	256	2016	2021+

Tabelle 5: Digitale Siegel

2.2 Terminal Authentisierung

Die Berechtigung zum Lesen und Schreiben von bestimmten Daten auf dem Chip muss ein Lesegerät über die Terminalauthentisierung nachweisen. Die Terminal Authentisierung basiert auf einer Public Key Infrastruktur bestehend aus einer *Country Verifying Certification Authority* als nationale Wurzelinstanz, einem *Document Verifier* für jeden Betreiber von Lesegeräten sowie den *Terminals*.

5 Die Umstellung erfolgt mit dem Wechsel der Schlüssellänge im übergeordneten CSCA-Zertifikat.

Das Signaturverfahren einschließlich der Schlüssellängen mit dem die kartenverifizierbaren Zertifikate (Card Verifiable Certificate) signiert werden, wird durch die Country Verifying Certification Authority festgelegt. Die Country Verifying Certification Authority wird vom BSI betrieben.

Tabelle 6 legt die zu verwendenden kryptographischen Verfahren verbindlich fest. Die Verwendungszeiträume beziehen sich auf die Zertifikatserzeugung.

Verfahren	*Algorithmus*	*Länge*	*Verwendung von*	*Verwendung bis*
Signatur	ECDSA	224 256	 2010	2010 2021+
Hash	SHA-224 SHA-256	224 256	 2010	2010 2021+

Tabelle 6: Terminal Authentisierung

2.3 Metadaten-Signer-Zertifikate

Die Hierarchie der Metadaten-Signer-Zertifikate besteht aus dem *MDS-Root-Zertifikat* als nationalem Vertrauensanker, den *MDS-SubCA-Zertifikaten* sowie den *MDS-Zertifikaten*, welche die Metadaten der Diensteanbieter signieren. Die Country Verifying Certificate Authority (CVCA) stellt zusätzlich zum CVCA Zertifikat und den DV-Zertifikaten, ein selbst signiertes MDS-Root-Zertifikat sowie MDS-SubCA-Zertifikate für die Document Verifier aus. Ein DV stellt für jeden bei ihm registrierten Diensteanbieter ein MDS-Zertifikat aus, sofern der Diensteanbieter eIDAS-Anwendungen anbietet. Erzeugung, Besitz und Nutzung der entsprechenden privaten Schlüssel erfolgt analog zu den privaten Schlüsseln der Terminal-Zertifikate. Für diesen Zweck werden in der CVCA-PKI zusätzliche X.509-Zertifikate (MDS-Zertifikate) ausgestellt.

2.3.1 MDS-Root- und MDS-SubCA-Zertifikate

Tabelle 7 legt die von der CVCAfür die Ausstellung von MDS-Root- und MDS-SubCA-Zertifikaten zu verwendenden kryptographischen Verfahren verbindlich fest. Die Verwendungszeiträume beziehen sich auf die Ausstellung der Zertifikate.

Verfahren	*Algorithmus*	*Länge*	*Verwendung von*	*Verwendung bis*
CVCA				
Signatur	ECDSA	384	2017	2021+
Hash	SHA-384	384	2017	2021+

Tabelle 7: MDS-Root- und MDS-SubCA-Zertifikate

2.3.2 MDS-Zertifikate

Tabelle 8 legt die von den DVs für die Ausstellung von MDS-Zertifikaten zu verwendenden kryptographischen Verfahren verbindlich fest. Die Verwendungszeiträume beziehen sich auf die Ausstellung der Zertifikate.

Verfahren	*Algorithmus*	*Länge*	*Verwendung von*	*Verwendung bis*
DV				
Signatur	ECDSA	256	2017	2021+
Hash	SHA-256	256	2017	2021+

Tabelle 8: MDS-Zertifikate

2.3.3 Signatur der Metadaten

Tabelle 9 legt die von Diensteanbietern für die Signatur von Metadaten zu verwendenden kryptographischen Verfahren verbindlich fest. Die Verwendungszeiträume beziehen sich auf die Ausstellung der jeweiligen Metadaten.

Verfahren	*Algorithmus*	*Länge*	*Verwendung von*	*Verwendung bis*
Diensteanbieter				
Signatur	ECDSA	256	2017	2021+
Hash	SHA-256	256	2017	2021+

Tabelle 9: Signatur von Metadaten

3 Zugriffskontrolle und sichere Kommunikation

Alle auf dem Chip gespeicherten Daten (mit Ausnahme einiger administrativer Daten) sind mit einem Schutz gegen unberechtigten Zugriff zu versehen.

3.1 Basic Access Control

Basic Access Control ist ein von der ICAO [4] standardisierter Zugriffsschutz. Dieses Verfahren basiert auf symmetrischer Kryptographie (die Schlüssel werden aus der maschinenlesbaren Zone erzeugt) und setzt keine Infrastruktur voraus. Basic Access Control ist für alle *Reisedokumente* zu implementieren. Langfristig ist es vorgesehen Basic Access Control durch PACE zu ersetzen, da PACE deutlich bessere kryptographische Eigenschaften besitzt.

Tabelle 10 legt die zu verwendenden kryptographischen Verfahren verbindlich fest.

Verfahren	***Algorithmus***	***Länge***	***Verwendung von***	***Verwendung bis***
Verschlüsselung	2-Key-3DES CBC-Mode	112	Vorgegeben durch [7].	
Integritätssicherung	3DES Retail MAC	112	Vorgegeben durch [7].	

Tabelle 10: Basic Access Control

3.2 PACE

PACE (Password Authenticated Connection Establishment) [13], [4] ist ein kryptographisches Verfahren mit den gleichen Zielen wie Basic Access Control, basiert aber auch auf asymmetrischer Kryptographie und kann mit mehreren, auch kurzen Passwörtern (PINs) verwendet werden.

Tabelle 11 legt die zu verwendenden kryptographischen Verfahren verbindlich fest. Die Verwendungszeiträume beziehen sich auf die Dokumentenausstellung.

Verfahren	***Algorithmus***	***Länge***	***Verwendung von***	***Verwendung bis***
Schlüsseleinigung	ECKA	256	2010	2021+
Permutation	AES CBC-Mode	128	2010	2021+
Mapping	Generic ECKA	256	2010	2021+
Verschlüsselung	AES CBC-Mode	128	2010	2021+
Integritätssicherung	AES CMAC	128	2010	2021+

Tabelle 11: PACE

3.3 Extended Access Control

Extended Access Control [5], [13] ist ein PKI-basiertes Zugriffskontrollverfahren, das sich aus den Bestandteilen Chip Authentisierung (s. Abschnitt 4.2) und Terminal Authentisierung (s. Abschnitt 2.2) zusammensetzt.

4 Identifikation des Ausweisdokuments

Das Ausweisdokument kann über die Dokumentennummer, die Chip Authentisierung oder die Restricted Identification identifiziert werden.

4.1 Dokumentennummer

Die Dokumentennummer bietet eine eindeutige Identifizierung des Dokumententyps. Die Dokumentennummer ist eine 9-stellige alphanumerische, pseudozufällige Nummer. Sie ist aus folgenden Zeichen zu bilden: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, C, F, G, H, J, K, L, M, N, P, R, T, V, W, X, Y, Z. Die Dokumentennummer kann zentral (beim Produzenten) oder dezentral erzeugt werden. Es wird empfohlen, die Dokumentennummer durch das Warbler-Verfahren aus einer sequentiell vergebenen Nummer zu erzeugen [24].

4.2 Chip Authentisierung

Die Chip Authentisierung [5], [13] ist ein kryptographisches Verfahren, mit dem die Echtheit des Chips durch den Aufbau einer starken Sitzungsverschlüsselung und -integritätssicherung nachgewiesen wird. Bei der Chip Authentisierung in Version 1 muss das Schlüsselpaar chipindividuell erzeugt werden, ab der Version 2 kann ein Schlüsselpaar für alle Dokumente einer Generation verwendet werden. Für die hoheitliche Nutzung muss zusätzlich ein chipindividuelles Schlüsselpaar verwendet werden.

4.2.1 Nationale Vorgaben

Für den Fall, dass die Chip Authentisierung in Version 1 für nationale Ausweisdokumente implementiert ist, legt Tabelle 12 die zu verwendenden kryptographischen Verfahren verbindlich fest. Die Verwendungszeiträume beziehen sich auf die Dokumentenausstellung.

Verfahren	***Algorithmus***	***Länge***	***Verwendung von***	***Verwendung bis***
Schlüsseleinigung	ECKA	256	2010	2021+
Verschlüsselung	2-Key-3DES CBC-Mode AES CBC-Mode	112 128	2010 3. Quartal 2012	3. Quartal 2012 2021+
Integritätssicherung	3DES Retail MAC AES CMAC	112 128	2010 3. Quartal 2012	3. Quartal 2012 2021+

Tabelle 12: Chip Authentisierung in Version 1 (Nationale Anwendung)

Tabelle 13 legt die zu verwendenden kryptographischen Verfahren für Chip Authentisierung in Version 2 verbindlich fest. Die Verwendungszeiträume beziehen sich auf die Dokumentenausstellung.

Verfahren	*Algorithmus*	*Länge*	*Verwendung von*	*Verwendung bis*
Schlüsseleinigung	ECKA	256	2010	2021+
Verschlüsselung	AES CBC-Mode	128	2010	2021+
Integritätssicherung	AES CMAC	128	2010	2021+

Tabelle 13: Chip Authentisierung in Version 2 (Nationale Anwendung)

4.2.2 Europäische Vorgaben

Tabelle 14 stellt die zu verwendenden kryptographischen Verfahren nach übergeordneten EU-Vorgaben dar. Diese müssen für Chip Authentisierung in Version 1 für den elektronischen Reisepass und den elektronischen Aufenthaltstitel zusätzlich zu den nationalen Vorgaben implementiert werden.

Verfahren	*Algorithmus*	*Länge*	*Verwendung von*	*Verwendung bis*
Verschlüsselung	2-Key-3DES CBC-Mode	112	2010	2019
Integritätssicherung	3DES Retail MAC	112	2010	2019

Tabelle 14: Chip Authentisierung (Europäische Vorgaben)

4.3 Restricted Identification

Die Restricted Identification [13] ist ein kryptographisches Verfahren zur Erzeugung von sektorspezifischen Kennungen.

Tabelle 15 legt die zu verwendenden kryptographischen Verfahren verbindlich fest. Die Verwendungszeiträume beziehen sich auf die Dokumentenausstellung.

Verfahren	*Algorithmus*	*Länge*	*Verwendung von*	*Verwendung bis*
Schlüsseleinigung	ECKA	256	2010	2021+
Hash zur Erzeugung von sektorspezifischen Kennungen	SHA-256	256	2010	2021+
Hash zur Erzeugung von Sperrsummen	SHA-256	256	2010	2021+

Tabelle 15: Restricted Identification

5 Qualifizierte elektronische Signatur

Sofern das Ausweisdokument eine Signaturfunktion unterstützt, muss diese als qualifizierte Signatur ausgestaltet sein. Es sind folgende Vorgaben einzuhalten.

5.1 Signaturerzeugung

Für die Signaturerzeugung sind die Vorgaben aus [25] einzuhalten. Tabelle 16 legt die zu verwendenden kryptographischen Verfahren darüber hinaus verbindlich fest. Die Verwendungszeiträume beziehen sich auf die Zertifikatsausstellung.

Verfahren	*Algorithmus*	*Länge*	*Verwendung von*	*Verwendung bis*
Signaturverfahren	ECDSA	256	2010	2021+
Hash	Der Hash ist extern zu berechnen. Dabei sind nach [25] geeignete Hashfunktionen mit einer Outputlänge von mindestens 256 Bit zu verwenden.			

Tabelle 16: Signaturerzeugung

5.2 Kennzeichnung der kryptographischen Verfahren

Die eSign-Anwendung wird durch eine Cryptographic Information Application ergänzt, die über die Verwendbarkeit des Signaturschlüssels Auskunft gibt. Es müssen folgende Object Identifier nach TR-03111 [14] zur Kennzeichnung der Verfahren verwendet werden:

- Signaturverfahren: `ecdsa-plain-signatures`
- Schlüssel in X.509 Zertifikaten: `id-ecPublicKey`
- Schlüssel im TLV-Format: `id-ecTLVPublicKey`

Das Signaturverfahren wird ohne Angabe des extern zu erzeugenden Hashes angegeben. Die Signaturanwendungskomponente kann die von der Karte erstellte Signatur im plain-Format in das X9.62-Format (einschließlich des verwendeten Hashes) umwandeln.

6 Profile

6.1 Elektronischer Reisepass

Der elektronische Reisepass beinhaltet die ePass-Anwendung [4].

6.1.1 Unterstützte Verfahren

Der elektronische Reisepass unterstützt folgende kryptographischen Verfahren:

- Passive Authentisierung
- Basic Access Control
- Extended Access Control Version 1
  - Chip Authentisierung 1
  - Terminal Authentisierung 1

Die zusätzliche Unterstützung von Password Authenticated Connection Establishment wird empfohlen. Ab 2013 muss PACE (gemäß [12]) vom elektronischen Reisepass unterstützt werden.

Die Absicherung der Kommunikation zwischen Chip und Lesegerät erfolgt über Secure Messaging, welches über Basic Access Control / Password Authenticated Connection Establishment und Chip Authentisierung vereinbart wird. Die Verwendung der Chip Authentisierung ist für den Leser nicht verpflichtend.

6.1.2 Nicht unterstützte Verfahren

Der elektronische Reisepass unterstützt keine Aktive Authentisierung.

6.2 Elektronischer Personalausweis

Der elektronische Personalausweis beinhaltet die folgenden drei Anwendungen: ePass [4], eID [13] und eSign [26].

6.2.1 Unterstützte Verfahren

Der elektronische Personalausweis unterstützt folgende kryptographischen Verfahren:

- Passive Authentisierung
- Password Authenticated Connection Establishment (gemäß [13])
- Extended Access Control Version 2
  - Chip Authentisierung 2
  - Terminal Authentisierung 2

- Restricted Identification
- Qualifizierte elektronische Signatur

Die Absicherung der Kommunikation zwischen Chip und Lesegerät erfolgt über Secure Messaging, welches über Password Authenticated Connection Establishment und Chip Authentisierung vereinbart wird. Alle Chips einer Generation müssen das gleiche Schlüsselpaar für die Chip Authentisierung verwenden, zusätzlich müssen chipindividuelle Schlüssel vorhanden sein.

6.2.2 Nicht unterstützte Verfahren

Der elektronische Personalausweis unterstützt folgende kryptographischen Verfahren nicht:

- Basic Access Control
- Extended Access Control Version 1
- Aktive Authentisierung

6.3 Elektronischer Aufenthaltstitel

Der elektronische Aufenthaltstitel beinhaltet die folgenden drei Anwendungen: ePass [4], eID [13] und eSign [26].

6.3.1 Unterstützte Verfahren

Der elektronische Aufenthaltstitel unterstützt folgende kryptographischen Verfahren:

- Passive Authentisierung
- Basic Access Control
- Password Authenticated Connection Establishment
- Extended Access Control (Version 1 und Version 2)
  - Chip Authentisierung 1 & 2
  - Terminal Authentisierung 1 & 2
- Restricted Identification
- Qualifizierte elektronische Signatur

Für den Zugriff auf die ePass-Anwendung kann Basic Access Control / Password Authenticated Connection Establishment (gemäß [12]) und bei Zugriff auf Fingerabdrücke Extended Access Control in Version 1 verwendet werden, für den Zugriff auf die eID- und eSign-Anwendung muss PACE (gemäß [13]) und Extended Access Control in Version 2 verwendet werden.

Alle Chips einer Generation müssen das gleiche Schlüsselpaar für die Chip Authentisierung verwenden, zusätzlich müssen chipindividuelle Schlüssel vorhanden sein.

6.3.2 Nicht unterstützte Verfahren

Der elektronische Aufenthaltstitel unterstützt keine Aktive Authentisierung.

6.4 Ankunftsnachweis

Der Ankunftsnachweis ist ein Papierdokument, das keinen Chip enthält. Der Ankunftsnachweis enthält ein gedrucktes digitales Siegel gemäß [27].

7 Zertifizierung der Ausweisdokumente

Die hoheitlichen Ausweisdokumente müssen nach den Common Criteria [28] zertifiziert sein. Das Common Criteria Zertifikat muss einen Hinweis enthalten, dass bei der Evaluierung des hoheitlichen Ausweisdokumentes die Anforderungen dieser Technischen Richtlinie berücksichtigt wurden.

7.1 Elektronischer Reisepass

Im Rahmen der erforderlichen Zertifizierung muss die Konformität zu folgenden Schutzprofilen nachgewiesen werden:

- BSI-CC-PP-0055-2009 (BAC [29]) und BSI-CC-PP-0087-V2-2016 (MR.ED [30]) oder
- BSI-CC-PP-0055-2009 (BAC [29]) und BSI-CC-PP-0056-V2-2012 (EAC mit PACE [31]).

Zudem wird empfohlen, die Konformität zum Schutzprofil [32] nachzuweisen.

Die Produktionsschritte *Initialisierung* und *Pre-Personalisierung* sind Teil des zu zertifizierenden Lebenszyklus des elektronischen Reisepasses. Die *Antennenmontage* ist nicht Teil des zu zertifizierenden Lebenszyklus, sofern diese nach der Initialisierung und der Pre-Personalisierung stattfindet.

Außerdem soll der Chip Maßnahmen vorsehen, so dass die Dauer eines erfolgreichen Brute-Force-Angriffs auf die MRZ im Durchschnitt 30 Tage nicht wesentlich unterschreitet.

7.2 Elektronischer Personalausweis

Im Rahmen der erforderlichen Zertifizierung muss die Konformität zu einem der folgenden Schutzprofile nachgewiesen werden:

- BSI-CC-PP-0087-V2-2016 [30] oder
- BSI-CC-PP-0061-2009 [33].

Zudem wird empfohlen, die Konformität zum Schutzprofil [32] nachzuweisen.

Die Produktionsschritte *Initialisierung und Pre-Personalisierung* sind Teil des zu zertifizierenden Lebenszyklus des elektronischen Personalausweises. Die *Antennenmontage* ist nicht Teil des zu zertifizierenden Lebenszyklus, sofern diese nach der Initialisierung und der Pre-Personalisierung stattfindet.

Die gespeicherten kryptographischen Schlüssel *Chip Authentication Private Keys*, *Restricted Identification Private Keys* und der *private Schlüssel für qualifizierte Signaturen* müssen durch geeignete Maßnahmen zusätzlich geschützt werden. Diese Maßnahmen sind im Einzelnen mit dem BSI abzustimmen.

Außerdem soll der Chip Maßnahmen vorsehen, so dass die Dauer eines erfolgreichen Brute-Force-Angriffs auf ein nicht-blockierendes Passwort (MRZ, CAN) im Durchschnitt 30 Tage nicht wesentlich unterschreitet.

7.3 Elektronischer Aufenthaltstitel

Im Rahmen der erforderlichen Zertifizierung muss die Konformität zu den folgenden Schutzprofilen nachgewiesen werden:

- BSI-CC-PP-0055-2009 (BAC [29]) und BSI-CC-PP-0087-V2-2016 (MR.ED [30]) oder

- BSI-CC-PP-0055-2009 (BAC [29]) und BSI-CC-PP-0069-2010 [34].

Zudem wird empfohlen, die Konformität zum Schutzprofil [32] nachzuweisen.

Die Produktionsschritte *Initialisierung* und *Pre-Personalisierung* sind Teil des zu zertifizierenden Lebenszyklus des elektronischen Aufenthaltstitels. Die *Antennenmontage* ist nicht Teil des zu zertifizierenden Lebenszyklus, sofern diese nach der Initialisierung und der Pre-Personalisierung stattfindet.

Die gespeicherten kryptographischen Schlüssel *Chip Authentication Private Keys*, *Restricted Identification Private Keys* und der *private Schlüssel für qualifizierte Signaturen* müssen durch geeignete Maßnahmen zusätzlich geschützt werden. Diese Maßnahmen sind im Einzelnen mit dem BSI abzustimmen.

Außerdem soll der Chip Maßnahmen vorsehen, so dass die Dauer eines erfolgreichen Brute-Force-Angriffs auf ein nicht-blockierendes Passwort (MRZ, CAN) im Durchschnitt 30 Tage nicht wesentlich unterschreitet.

8 Terminals

Dieses Kapitel enthält Empfehlungen für Terminals, die mit einem hoheitlichen Dokument kommunizieren. Diese sind für nach Common Criteria zertifizierte Lesegeräte verbindlich zu beachten. Das Zertifikat kann einen Hinweis enthalten, dass die Anforderungen dieser Richtlinie erfüllt wurden.

8.1 Algorithmen und Schlüssellängen

Die durch ein Terminal mindestens zu unterstützenden Algorithmen und Schlüssellängen ergeben sich aus den zu unterstützenden Dokumenten.

8.2 Basic Access Control

Basic Access Control sollte vom Terminal nur dann verwendet werden, wenn das auszulesende Dokument die Verwendung von PACE nicht unterstützt.

8.3 PACE

Für die Erzeugung der notwendigen ephemeralen Schlüssel ist ein Zufallszahlengenerator aus einer der folgenden Klassen (siehe [22]) zu verwenden:

- DRG.2 oder höher,
- PTG.2 oder höher,
- NTG.1.

8.4 Terminal- und Chipauthentisierung

Für die Erzeugung der Nonce für die Signaturerzeugung als Bestandteil der Terminalauthentisierung und die Erzeugung des ephemeralen Schlüssels für die Chipauthentisierung ist ein Zufallszahlengenerator aus einer der folgenden Klassen (siehe [22]) zu verwenden:

- DRG.3 oder höher,
- PTG.2 oder höher,
- NTG.1.

Literaturverzeichnis

[1] BSI TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2018-01, 2018

[2] Das Europäische Parlament und der Rat der Europäischen Union, VERORDNUNG (EU) Nr. 910/2014 der Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (http://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:32014R0910), , 23. Juli 2014

[3] Europäische Kommission , DURCHFÜHRUNGSVERORDNUNG (EU) 2015/1501 DER KOMMISSION vom 8. September 2015 über den Interoperabilitätsrahmen gemäß Artikel 12 Absatz 8 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, 2015

[4] ICAO 9303, Machine Readable Travel Documents, 7th edition, 2015

[5] BSI TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 1, Version 2.20, 2015

[6] Rat der EU, Standards for security features and biometrics in passports and travel documents issued by Member States, Council Regulation (EC) No 2252/2004, 13. Dezember 2004

[7] EU Kommission, Technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States, Commission Decision C(2006) 2909, 28. Juni 2006

[8] EU Kommission, Technical specifications for the uniform format for residence permits for third country nationals, Commission Decision C(2011) 5478, 4. August 2011

[9] EU Kommission, Amendment to C(2011) 2909 laying down the technical specifications on the standards for security features and biometrics in passports and travel documents issued by member states, Commission Decision C(2011) 5499, 4. August 2011

[10] EU Kommission, Amendment to Commission Decision C(2002) 3069 laying down the technical specifications for the uniform format for residence permits for third country nationals, Commission Decision C(2013) 6178, 30. September 2013

[11] EU Kommission, Amendment to C(2006) 2909 final laying down the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States and C(2008) 8657 laying down a certificate policy as required in the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States and updating the normative reference documents, Commission Decision C(2013) 6181, 30. September 2013

[12] ICAO Technical Report, Supplemental Access Control for Machine Readable Travel Documents, Version 1.01, 2010

[13] BSI TR-03110-2, Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 2, Version 2.21, 2016

[14] BSI TR-03111, Elliptic Curve Cryptography (ECC) Version 2.0, 2012

[15] NIST FIPS PUB 197, Specification for the Advanced Encryption Standard (AES), 2001

[16] ISO/IEC 10116:2006, Information technology - Security techniques - Modes of operation for an n-bit block cipher, 2006

[17] NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005

[18] NIST Special Publication 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Revision 1, 2012

[19] ISO/IEC 9797-1:2011, Information technology - Security techniques - Message Authentication Codes (MACs), Part 1: Mechanisms using a block cipher, 2011

[20] NIST FIPS PUB 180-4, Secure Hash Standard (SHS), 2015

[21] IETF RFC 5639, M. Lochter, J. Merkle, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, 2010

[22] BSI AIS 20/31, A proposal for: Functionality classes for random number generators, Version 2.0, 2011

[23] eIDAS Technical Subgroup, eIDAS Technical Specifications - Interoperability Architecture,

[24] Margraf, Marian, Beschreibung und Einsatz der Verschlüsselungsfunktion Warbler, 2006

[25] SOG-IS , Agreed Cryptographic Mechanisms, Version 1.0, Stand 2016,

[27] BSI TR-03117, eCards mit kontaktloser Schnittstelle als sichere Signaturerstellungseinheit, 2017

[28] BSI TR-03137, Optically Verifiable Cryptographic Protection of non-electronic Documents (Digital Seal), Version 2.0, 2015

[29] Common Criteria, Common Critera for Information Technology Evaluation Security, Parts 1-3

[29] BSI CC-PP-0055, Machine Readable Travel Document with "ICAO Application" Basic Access Control, 2009

[30] BSI CC-PP-0087, Common Criteria Protection Profile BSI-CC-PP-0087, Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use (MR.ED-PP),

[31] BSI CC-PP-0056, Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE, 2012

[32] BSI CC-PP-0090, Common Criteria Protection CC-PP-0090 - Profile Configuration Machine Readable Electronic Documents - Optionales Nachladen (MR.ED-ON-PP),

[34] BSI CC-PP-0061-2009, Common Criteria Protection Profile - Electronic Identity Card (ID_Card PP) Version 1.03, 2009

[34] BSI CC-PP-0069-2010, Common Criteria Protection Profile Electronic Residence Permit Card (RP_Card PP), 2010