Bundesamt
für Sicherheit in der
Informationstechnik

Identifikation relevanter Testfälle für das Sicherheitsmodul nach BSI TR-03109-2

BSI TR-03109-TS-2-Testidentifikation

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

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

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 „Identifikation relevanter Testfälle für das Sicherheitsmodul nach BSI TR-03109-2“ bildet den zweiten von insgesamt drei Teilen der „Testspezifikation zur Prüfung des Sicherheitsmoduls nach BSI TR-03109-2“ ([BSI TR-03109-TS-2]). Es dient der Identifikation 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 folgt:

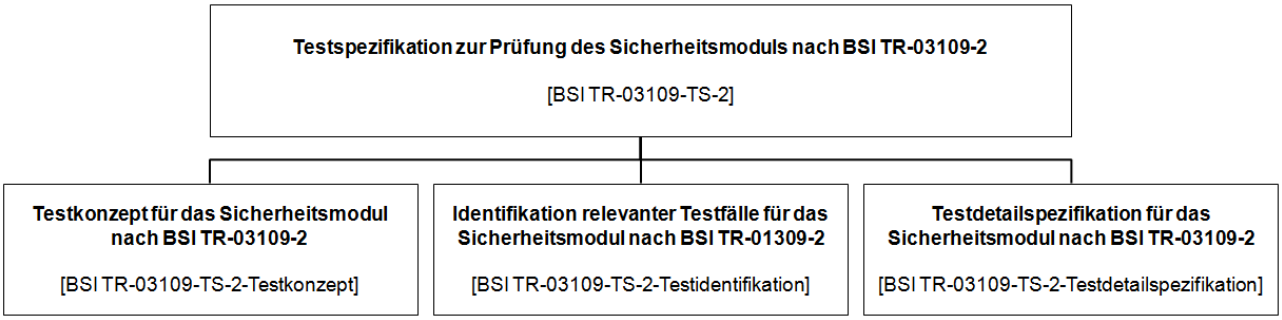

Abbildung 1: Aufbau der Testspezifikation

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

   Auf Basis des im Dokument Testkonzept ([BSI TR-03109-TS-2-Testkonzept]) beschriebenen Testkonzepts für die Konformitätsprüfung eines Sicherheitsmoduls wird im vorliegenden Dokument Testidentifikation genauer dargestellt, was bzw. welche Anforderungen an ein

Sicherheitsmodul aus der Technischen Richtlinie [BSI TR-03109-2] getestet werden sollen.

Das vorliegende Dokument Testidentifikation sowie das zugehörige Dokument [BSI TR-03109-TS-2-TF] mit Übersichtstabellen über die Testfälle zeigen somit insgesamt auf, was im Rahmen der TR-03109-TS-2 zu testen ist.

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

   Das Dokument (bzw. seine XML-Datei) zeigt somit auf, wie die im vorliegenden Dokument Testidentifikation identifizierten, generisch beschriebenen Testfälle konkret umzusetzen sind.

1.1 Zielsetzung

Das Dokument Testidentifikation mit seinem zugehörigen Dokument [BSI TR-03109-TS-2-TF] dient der Zusammenstellung und Beschreibung der für die Konformitätsprüfung eines Sicherheitsmoduls gegen die funktionalen Vorgaben der Technischen Richtlinie [BSI TR-03109-2] relevanten Testfälle.

1.2 Bezugsdokumente

Das vorliegende Dokument beinhaltet die Identifikation relevanter Testfälle für gemäß der Technischen Richtlinie [BSI TR-03109-2] entwickelte Sicherheitsmodule.

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

1.3 Begriffe, Terminologie

Der Begriff der Konformitätsprüfung eines Sicherheitsmoduls umfasst die Prüfung eines solchen Sicherheitsmoduls bzgl. seiner Konformität zu den funktionalen Anforderungen der technischen Spezifikation von Sicherheitsmodulen in der Technischen Richtlinie [BSI TR-03109-2].

Die Überprüfung von Dokumenten oder die Überprüfung des Prüfgegenstandes nach seiner Dokumentation wird als Prüfung bezeichnet.

Einzelne Prüf- bzw. Testfälle des im Rahmen des Dokumentes beschriebenen Testwerkzeugs bzw. Testtools sowie die in der Testdetailspezifikation ([BSI TR-03109-TS-2-Testdetailspezifikation]) beschriebenen Prüfungen und Tests werden Test oder Testfall genannt.

Um auf den Ausdruck „und/oder“ zu verzichten, wird „oder“ im gesamten Dokument nicht als exklusives „oder“ und damit in der Form von „entweder oder“ sondern als inklusives „oder“ und damit in der Art verwendet, dass beide durch das „oder“ getrennte Optionen möglich sind.

1.4 Versionshistorie

Version	Datum	Änderungen
1.0	06.03.2018	Finale Version / Erstausgabe

Tabelle 1: Versionshistorie

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-TF: BSI-TR-03109-TS-2-TF-Identifizierung_SM_V1.0.zip, Version 1.0, 2018, Bundesamt für Sicherheit in der Informationstechnik

BSI TR-03109-TS-2-Testdetailspezifikation: Testdetailspezifikation für das Sicherheitsmodul nach BSI TR-03109-2, V1.0, 2018, Bundesamt für Sicherheit in der Informationstechnik

Abkürzungsverzeichnis

Abkürzung	Beschreibung
APDU	Application Protocol Data Unit
API	Application Programming Interface
CAPDU	Command Application Protocol Data Unit
CC	Common Criteria
CLA	Class
EMT	Externe Marktteilnehmer
GWA	Gateway Administrator
HAN	Home Area Network
I^2C	Inter-Integrated Circuit
INS	Instruction
LMN	Local Metrological Network
MAC	Message Authentication Code
PIN	Personal Identification Number
PP	Protection Profile
RAPDU	Response Application Protocol Data Unit
SM	Security Module
SMGW	Smart Meter Gateway
TLV	Tag Length Value
TR	Technische Richtlinie
TS	Testspezifikation
WAN	Wide Area Network
XML	Extensible Markup Language

Tabelle 2: Abkürzungen