Bundesamt
für Sicherheit in der
Informationstechnik

Testkonzept zu BSI TR-03109-TS-1

zu: BSI TR-03109 - Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen

Version: 00.91
Datum : 30.01.2015

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: smartmeter@bsi.bund.de
Internet: https://www.bsi.bund.de

Hinweis zu Version 00.91

Das vorliegende Dokument ist ein Arbeitsergebnis des Projektes zur Erstellung der Testspezifikation für [BSI TR-03109-1]. Im weiteren Projektverlauf werden Festlegungen dieser Konzeption präzisiert und ggf. auch abgeändert. Dies soll sowohl bei der Rezeption als auch bei sonstiger Verwendung außerhalb des Projektkontextes berücksichtigt werden.

Die im Konzept getroffenen Aussagen müssen insofern auch nicht in jedem Falle die Auffassung des Herausgebers der Technischen Richtlinie wiedergeben.

Dokumentkonventionen

Dieser Abschnitt erläutert die Festlegungen zur Gestaltung des Dokumentes.

Hinweis: Es ist zwischen Vereinbarungen für die Erstellungsphase (Dokumentenentwurfsphase) und Vereinbarungen für das (ggf.) zu veröffentlichende Dokument zu unterscheiden.

Dateiname(n):

Dateinamen sind (in der Vorveröffentlichungsphase) wie folgt aufgebaut:

`{TR-ID}_{Arbeitspaket(Projekt)}_{Dokumenttyp}_V{0X.YZ}.{Erweiterung}`

Beispiel für das vorliegende Dokument:

`TR-03109-TS-1_AP2-2_Testkonzept_V0.90.4.odt`

Markierungs- und Formatierungslegende:

{___} ... Platzhalter → durch geschweifte Klammern um drei Unterstriche kenntlich gemacht, zusätzlich grau (RGB(230,230,230)) hinterlegt

Markierungs- und Formatierungslegende für die Dokumenterstellungsphase:

Absätze, die ausschließlich für die Konzeptionsphase bis Projekt-Arbeitspaket 3 Gültigkeit haben, sind grau hinterlegt dargestellt und von der Zeilennummerierung ausgeschlossen:

Dieser Absatz beschreibt ein Vorgehen oder eine Festlegung für die Erstellung von Konzept oder Spezifikation, ist jedoch nicht für die Veröffentlichung in der finalen Version der Testspezifikation vorgesehen.

→ Benutzervorlage „Projektbezogen“

Hinweis zum Tempus in Absätzen, die für die Veröffentlichung vorgesehen sind:

Wenn es für die Veröffentlichung erforderlich ist, auf zu diesem zukünftigen Zeitpunkt abgeschlossene Aktivitäten zu verweisen, erfolgt die Formulierung im Präteritum. Dies dient ausschließlich dazu, eine explizite Aufarbeitung unmittelbar vor der Veröffentlichung zu vermeiden und trifft keine Aussage bezüglich des tatsächlichen Vorliegens von Projektergebnissen.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in der Technische Richtlinie (TR) [BSI TR-03109-1] die Anforderungen an die Funktionalität, Interoperabilität und Informationssicherheit von Kommunikationseinheiten intelligenter Messsysteme („Smart Meter Gateways“ (SMGW)) festgelegt.

Smart Meter Gateways, die zukünftig in Deutschland installiert werden, müssen diese Richtlinie berücksichtigen und alle Anforderungen der Richtlinie korrekt implementieren. Dadurch soll sichergestellt werden, dass Smart Meter Gateways unterschiedlicher Hersteller wie in der Richtlinie spezifiziert zueinander kompatibel sind und über die in der TR geforderte Funktionalität verfügen.

Kapitel 1 erläutert den Kontext der Testspezifikation (TS). Es werden Zielsetzung (Kapitel 1.1) und Zielgruppen (Kapitel 1.2) beschrieben und darüber hinaus in Kapitel 1.3 diejenigen Dokumente aufgelistet, die im Zusammenhang zum Testkonzept stehen. Kapitel 1.4 erklärt die verwendeten Begriffe und Terminologien.

Am Ende des Kapitels findet sich die Änderungshistorie.[1]

1.1 Zielsetzung

Dieses Kapitel (1.1) hat informativen Charakter.

Die vorliegende Testspezifikation definiert das Testvorgehen und die Testinhalte für den Konformitätstest gemäß [BSI TR-03109-1]. Ziel dieses Tests ist es, sowohl Herstellern als auch zukünftigen Nutzern von SMGW von unabhängiger Seite eine Bestätigung darüber zu erteilen, dass die in Verkehr zu bringende Komponente auf die Erfüllung der Anforderungen laut [BSI TR-03109-1] überprüft wurde und das Ergebnis zu diesen Anforderungen konform ist.

Die Testspezifikation soll auch sicherstellen, dass unabhängig von der testenden Prüfstelle die Ergebnisse für ein und dasselbe Testobjekt gleich ausfallen.

Nachfolgende Grundsätze gelten für die Testergebnisse, die anhand der Testspezifikation [BSI TR-03109-TS-1] erzielt werden sollen:

Objektivität

Ein Testergebnis muss mit einem Minimum an subjektivem Urteil oder subjektiver Meinung erzielt werden. Die Objektivität wird u. a. auch durch eindeutige Testfälle und der dafür zu einem späteren Zeitpunkt entwickelten Testwerkzeuge erzielt.

Unvoreingenommenheit

Ein Testergebnis darf niemals schon vor der eigentlichen Testdurchführung feststehen und muss frei von (positiven oder negativen) Vorurteilen sein.

Wiederholbarkeit

Ein erneuter Test derselben Systemkomponente mittels eines Testwerkzeugs durch dieselbe Prüfstelle muss zur gleichen Gesamtbewertung führen wie der erste Test.

Reproduzierbarkeit

Ein Test derselben Systemkomponente mittels eines Testwerkzeugs durch eine andere Prüfstelle muss zur gleichen Gesamtbewertung führen wie der erste Test.

Die Testspezifikation definiert nicht, zu welchem Anlass (Ersteinführung, Aktualisierung, Fertigungslose etc.) ein SMGW-Produkt Konformitätstests zu unterziehen ist.[2]

1 In Kapitel 1 wird für die Veröffentlichung der TS auch die fachlich zuständige Stelle zu benennen sein.

2 vgl. Hinweis in [**TSE-TA**], Punkt 1.3: Es wird empfohlen, dahingehende Festlegungen in einem dedizierten Dokument zu treffen und mit allen (relevanten) Prüfvorschriften im SMGW-Umfeld zu synchronisieren.

1.2 Zielgruppe

Die Testspezifikation [BSI TR-03109-TS-1] richtet sich an die Beteiligten an Konformitätstests von SMGW nach [BSI TR-03109-1], insbesondere

- Hersteller von SMGW, die ein SMGW-Produkt einer Prüfung unterziehen wollen und
- anerkannte Prüfstellen und akkreditierte Prüfstellen, die in Vorbereitung einer Zertifizierung die Tests gemäß der Testspezifikation vornehmen und die Ergebnisse bewerten.

Tests auf Konformität mit den Anforderungen der [BSI TR-03109-1] müssen die in dieser Testspezifikation festgelegten Testfälle vollständig beinhalten.

1.3 Bezugsdokumente

Dieses Kapitel (1.3) hat informativen Charakter.

[BSI TR-03109-1] legt die zu verwendenden Bezugsdokumente verbindlich fest. Kapitel 1.3 erläutert diese Bezugsdokumentation im Hinblick auf ihre Anwendung für die Testspezifikation.

Die vorliegende Testspezifikation Smart Meter Gateway [BSI TR-03109-TS-1] ist direkt der Technischen Richtlinie [BSI TR-03109-1] untergeordnet.

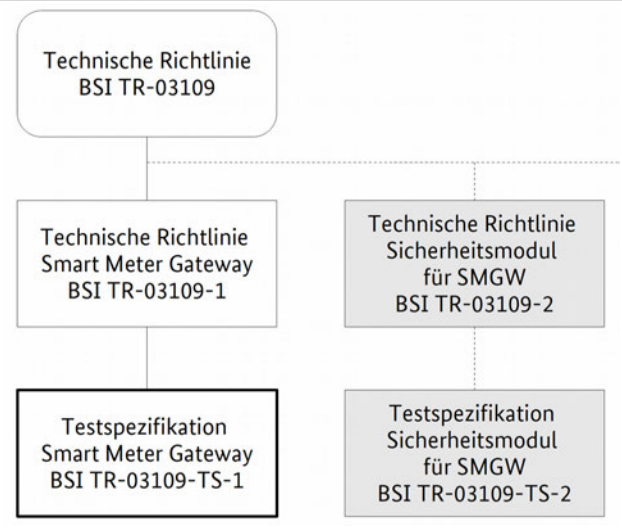

Abbildung 1: Dokumentenkontext BSI TR-03109 (Ausschnitt)

[BSI TR-03109-1] ist wie die Richtlinien für Sicherheitsmodule für SMGW [BSI TR-03109-2], Kryptographische Vorgaben für SMGW [BSI TR-03109-3] sowie Public Key Infrastruktur für SMGW [BSI TR-03109-4] und Kommunikationsadapter (in Vorbereitung) der Technischen Richtlinie [BSI TR-03109] nachgeordnet.

Abbildung 1 zeigt ausschnittsweise die Zuordnung der TS zum Dokumentenkontext [BSI TR-03109].

Die Technische Richtlinie [BSI TR-03109-1] verweist auf eine Reihe von Anlagen, welche in der Richtlinie definierte Anforderungen konkretisieren. Abbildung 2 gibt einen Überblick zu den Anforderungsquellen, die sich aus [BSI TR-03109-1] ergeben und weist auf den Kontext zu [GW_PP] hin.

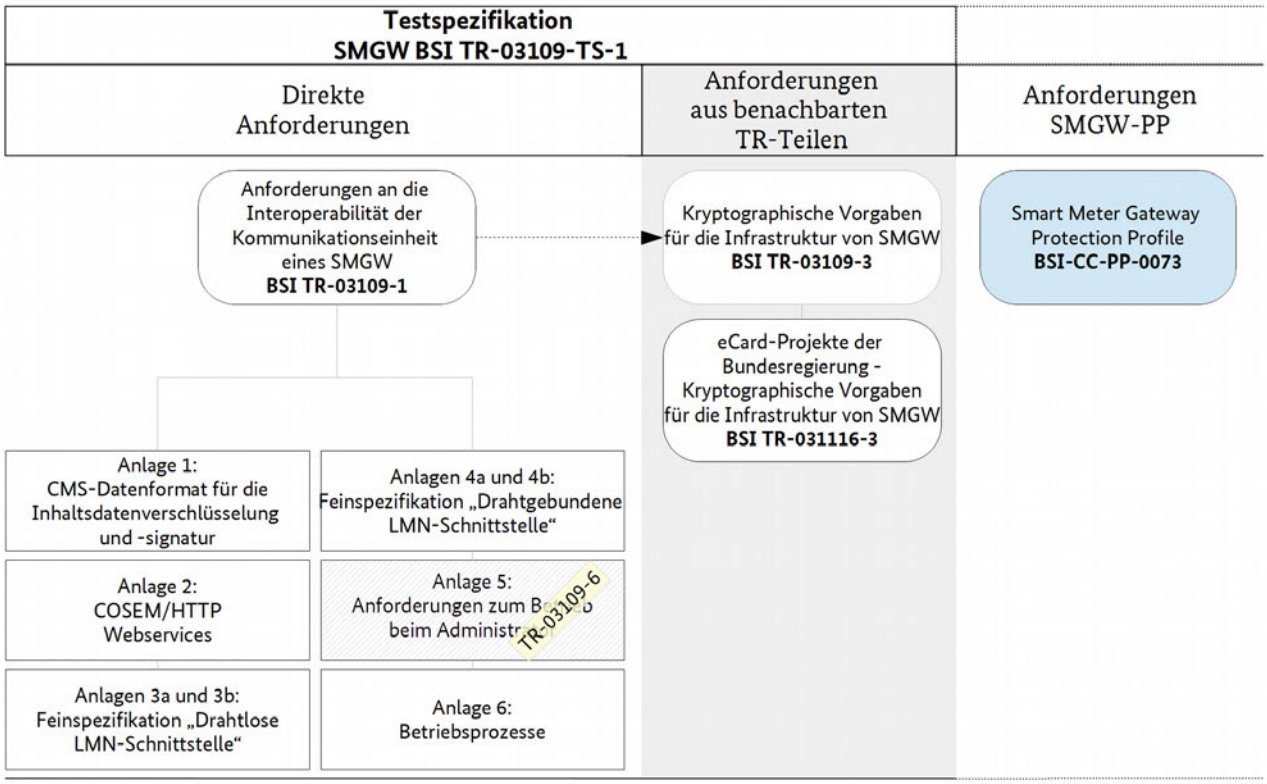

Abbildung 2: Übersicht Anforderungsquellen [BSI TR-03109-1]

Das vorliegende Dokument referenziert auf Anforderungen aus [BSI TR-03109], stellt jedoch selbst keine darüber hinausgehenden Anforderungen an ein SMGW auf.

Die Testspezifikation bezieht sich stets auf eine konkrete Version der [BSI TR-03109-1], die im Literatur- und Referenzverzeichnis benannt ist.Einzelne Bezugsdokumente (Richtlinien, Normen, Standards), die für die Erstellung der Testspezifikation von besonderer Bedeutung sind, werden nachfolgend erläutert.

1.3.1 Anlagen zu [BSI TR-03109-1]

Tabelle 1 führt die geltenden Anlagen zu [BSI TR-03109-1] im Einzelnen auf und weist auf eventuelle Besonderheiten der aktuellen Version hin.

Kurzbezeichnung	Titel	Versionshinweise
[BSI TR-03109-1/AI]	CMS-Datenformat für die Inhaltsdaten-verschlüsselung und Signatur	Eine Überarbeitung ist in Vorbereitung.
[BSI TR-03109-1/AII]	COSEM/HTTP Webservices	Diese Anlage befindet sich in Bearbeitung.
[BSI TR-03109-1/AIIIa]	Feinspezifikation „Drahtlose LMN-Schnittstelle“ Teil a: „OMS Specification Volume 2, Primary Communication“	Die Feinspezifikation drahtlose LMN-Schnittstelle ist in der aktuellen Version 4.0.2 als ein Dokument für Anlage IIIa und IIIb geführt.
[BSI TR-03109-1/AIIIb]	Feinspezifikation „Drahtlose LMN-Schnittstelle“ Teil b: „OMS Technical Report Security“	
[BSI TR-03109-1/AIVa]	Feinspezifikation „Drahtgebundene LMN-Schnittstelle“ Teil a: „HDLC für LMN“	Ein Überarbeitung basierend auf dem FNN Lastenheft Leitungsgebundene LMN-Protokolle 1.0 (Dokument ist noch nicht final) ist in Vorbereitung
[BSI TR-03109-1/AIVb]	Feinspezifikation „Drahtgebundene LMN-Schnittstelle“ Teil b: „SML – Smart Message Language“	
[BSI TR-03109-1/AV]	Anforderungen zum Betrieb beim Administrator	Diese Anlage soll in eine eigenständige TR-03109-6 überführt werden.
[BSI TR-03109-1/AVI]	Betriebsprozesse	-

Tabelle 1: Anlagen zu [BSI TR-03109-1]

69 1.3.1.1 In [BSI TR-03109-3] referenzierte normative Dokumente

70 [BSI TR-03109-3] referenziert auf in Tabelle 2 aufgeführte Richtlinien bzw. Standards.

Kurzbezeichnung	Titel	Versionshinweise
BSI TR-03116, Teil 3 [BSI TR-03116-3]	eCard-Projekte der Bundesregierung - Kryptographische Vorgaben für die Infra-struktur von intelligenten Messsystemen“	Version 2014

Tabelle 2: Referenzen gemäß [BSI TR-03109-3]

Entwürfe für Testspezifikationen

Nachfolgende TS-Entwürfe lagen bei Erstellung des vorliegenden Dokumentes vor und wurden nach Möglichkeit berücksichtigt:

(1) Konzept einer Testsystemarchitektur VDE (17.4.14 / ohne Version)[TSE-VDE],

(2) Prüfkonzept secuvera (15.4.2014 / V.1) [TSE-SV],

(3) Testkonzept TÜVIT/achelos (ohne Datum / ohne Version) [TSE-TA],

(4) Prüfkonzept mtg (17.4.2014 / Version 0.2.1) [TSE-MT]

71 1.4 Begriffe, Terminologie

72 Mit Ausnahme der Zusammenstellung in Tabelle 5 hat dieses Kapitel (1.4) informativen Charakter.

73 Wenn in der vorliegenden TS auf Aktivitäten Bezug genommen wird, die im Rahmen einer Prüfung von
74 SMGW gemäß [BSI TR-03109] und [GW_PP] erfolgen, werden diese als → Prüfverfahren bezeichnet.

75 Aktivitäten, die sich aus [BSI TR-03109-1] konkret wie in der vorliegenden Spezifikation beschrieben
76 ergeben, werden als → Test bezeichnet.

77 Als Referenzpunkt für testspezifische Begriffe werden die Definitionen laut Version 2.3 aus dem [ISTQB®-
78 Glossar] verwendet.

79 Die Regelung zur Verbindlichkeit von Anforderungen in Anlehnung an RFC2119 wird gleichlautend wie in
80 [BSI TR-03109-1] festgelegt verwendet.

81 Von zentraler Bedeutung für die Testspezifikation sind folgende Begriffe, die in [M441-TR] vereinbart sind:

Begriff[3]	**Definition**
Konformität	*Erfüllung der festgelegten Anforderungen durch ein Produkt, einen Prozess oder einen Dienst*
Conformance	Fulfillment of a product, process or service of specified requirements.
Funktion	*Prozess, der ununterbrochen oder in bestimmten Abständen, selbsttätig oder auf Anfrage bestimmte Handlungen ausführt, wie Datenerfassung, Auslesen eines Datensatzes, Überprüfen oder Ändern eines Zustandes oder Betätigen eines Schalters; eine Anwendung setzt sich zusammen aus einer Funktion oder mehreren Funktionen; eine Funktion kann grundlegend oder wahlfrei sein*
Function	Process which constantly or at defined intervals, automatically or on demand, performs specific activities such as sampling data, reading a data set, verifying or changing a status, or activating a switch. An application is composed of one or more functions. A function can be basic or optional.
Interoperabilität	*Fähigkeit eines Systems zum Datenaustausch mit anderen Systemen eines anderen Typs und/oder von anderen Herstellern*
Interoperability	Ability of a system to exchange data with other systems of different types and/or from different manufacturers.

Tabelle 3: Begriffsdefinitionen aus [M441-TR][4]

82 Für den Begriff „Funktionalität“ wird auf die Definition der ISO/IEC 25010:2011[5] für Qualitätsmerkmale
83 zurückgegriffen, die funktionale Angemessenheit in folgende Untermerkmale gliedert:

Begriff	**Definition**
Merkmalsgruppe: Funktionale Angemessenheit	Ausmaß, in dem das Produkt / System Funktionen anbietet, die festgelegte und vorausgesetzte Erfordernisse unter spezifizierten Bedingungen erfüllen.
Funktionale Vollständigkeit	Ausmaß, zu dem der Funktionsumfang alle festgelegten Aufgaben und Nutzerzielsetzungen abdeckt.
Funktionale Korrektheit	Ausmaß, zu dem das Produkt / System korrekte Ergebnisse mit dem nötigen Ausmaß an Präzision liefert.
Funktionale Eignung	Ausmaß, zu dem die Funktionen das Erreichen festgelegter Aufgaben und Zielsetzungen unterstützen.

Tabelle 4: Funktionalitätsmerkmale nach ISO/IEC 25010:2011

3 Die Übersetzung ist gleichlaufend mit der Fortschreibung der Richtlinie an DIN/CEN/CLC/ETSI/TR 50572 (VDE0418-0):2014-10 anzupassen.

4 Verbindlich für [BSI TR-03109] und nachgeordnete Dokumente in Version 1.0 ist die englische Fassung der Begriffsdefinitionen. Die deutsche Übersetzung folgt DIN CEN/CLC/ETSI/TR 50572 (VDE 0418-0).

5 Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models, First Edition 2011-03-01

84 Nachstehend werden die in der Testspezifikation zusätzlich normativ verwendeten Begriffe definiert.

Begriff	Definition
Testsuite	Ergänzend zu der Definition des [ISTQB®-Glossar][6] wird unter einer Testsuite die vollständige Zusammenstellung von – teilweise oder ganz automatisiert – ausführbaren Testfällen für definierte Testelement-Gruppen verstanden. Vgl. zu Testsuite auch: Ausführungen in Kapitel 2.4
Webservice-Anbieter (WS-Anbieter)	Entität, die einen Webservice als Dienst anbietet. Anmerkung: Zur Vermeidung von begrifflichen Überschneidungen wird auf den gebräuchlichen Begriff „Webservice-Provider“ verzichtet.
Webservice-Benutzer (WS-Benutzer)	Entität, die einen Webservice aktiv nachfragend nutzt. Anmerkung: Zur Vermeidung begrifflicher Überschneidungen wird auf den oft gebräuchlichen Begriff „Webservice-Consumer“ verzichtet.

Tabelle 5: Begriffsdefinitionen mit normativem Charakter für die TS

85 1.5 Versionshistorie

Version	Datum	Beschreibung
0.40	21.07.2014	Abstimmungsversion intern (T-Systems, AP 1-1)
0.50	09.09.2014	Reviewversion intern (BSI)
0.60 ... 0.74	14.10.2014	Korrekturversionen intern (T-Systems, AP1-2)
0.75	14.10.2014	Überarbeitung nach Review BSI
0.80	22.10.2014	Reviewversion intern (BSI)
0.90	24.10.2014	Korrekturversion (T-Systems, Abschluss AP1)
0.91	30.01.2015	formale Korrekturen und Ergänzungen zur Verbesserung der Zugänglichkeit

Tabelle 6: Versionshistorie

86

6 Die deutsche Übersetzung der Definition lautet: „Die Zusammenstellung (Aggregation) mehrerer Testfälle für den Test einer Komponente oder eines Systems, bei der Nachbedingungen des einen Tests als Vorbedingungen des folgenden Tests genutzt werden können.“

2 Technische Einleitung

Dieses Kapitel

- schildert die Ausgangssituation für die durchzuführenden Tests,
- grenzt das Testobjekt ab und gliedert es in Testelemente (2.1.1 Testobjekt, Testelemente),
- erläutert das grundsätzliche Vorgehen (2.1.2 Bewertungskriterien für Testelemente, 2.2 Testverfahren),
- definiert die Rahmenbedingungen (2.3 Testeingangskriterien für das Testobjekt, 2.5 Testabgrenzung) und
- zeigt den grundsätzlichen Aufbau eines Testfalls der [BSI TR-03109-TS-1].

Darüber hinaus wird in 2.6 Testinfrastruktur, Testumgebung der Zusammenhang zu testumgebungsspezifischen Festlegungen hergestellt.

Allgemein beschreibt Kapitel 2 das der TS zugrunde liegende Testvorgehen und erläutert Testfall- und Testszenario-übergreifende Festlegungen.

Der Prüfprozess wird in Bezug auf die Testaktivitäten, die zur Durchführung der in [BSI TR-03109-TS-1] definierten Tests erforderlich sind, dem fundamentalen Testprozess folgen, welcher die Aktivitäten

- Planung und Steuerung,
- Analyse und Design,
- Realisierung und Durchführung,
- Bewertung und Berichterstattung sowie
- den Abschluss der Testaktivitäten

umfasst. Die Ausgestaltung dieser Aktivitäten wird ausschließlich in Bezug auf die spezifischen Erfordernisse der [BSI TR-03109-TS-1] beschrieben. Die vorliegende TS deckt im fundamentalen Testprozess die Arbeitsergebnisse der Phase Analyse und Design und in Bezug auf die Testfälle und -daten bis zur Erstellung der konkreten Testfälle die Phase Realisierung und Durchführung ab. Ausgenommen sind für beide Testphasen konkrete Testinfrastrukturvorgaben.

Übergreifende Aspekte des Prüfprozesses, wie z. B. die Anerkennung als Prüfstelle und die im Rahmen des Prüfprozesses neben den Tests erforderlichen Aktivitäten und andere Testprozessphasen, wie z. B. Planung und Steuerung, sind nicht Gegenstand des Dokuments.

Testfälle zu einem oder ggf. auch mehreren Testelementen sollen in Testsuiten zusammengefasst werden.

Die konkreten Inhalte für die Testsuite(n) werden in AP 2 und AP 3 definiert.

Anmerkung: Kapitel 5 enthält Hinweise und Empfehlungen, die bei der Planung und Durchführung von Tests gemäß der TS beachtet werden sollen.

2.1 Ausgangssituation

Dieses Kapitel (2.1) hat informativen Charakter.

Kapitel 2.1 erläutert den Ausgangspunkt der vorliegenden Testspezifikation. Insbesondere wird das Testobjekt beschrieben und detailliert (2.1.1) sowie die Kriterien dargestellt, anhand derer für die Testelemente Konformitätstests spezifiziert wurden (2.1.2).

Die Anforderungen der [BSI TR-03109] an SMGW sind herstellerunabhängig formuliert. Um die geforderte Interoperabilität und Funktionalität der Kommunikationseinheit von SMGW-Produkten sicherzustellen, sind Konformitätstest erfolgreich durchzuführen.

Folgende Aspekte werden durch die in der TS beschriebenen Konformitätstests abgedeckt:

- Die Gesamtheit der Testfälle verifiziert ausschließlich die Erfüllung von in [BSI TR-03109-1] spezifizierten Anforderungen.
- Die Testfälle sind so entworfen, dass soweit technisch machbar eine Automatisierung der Testdurchführung möglich ist.

2.1.1 Testobjekt, Testelemente

Testobjekt für Tests gemäß der vorliegenden TS ist ein jeweils gemäß den Testeingangskriterien lt. Kapitel 2.3 dokumentiertes SMGW.

Orientiert an den Vorgaben der [BSI TR-03109-1] wird das Testobjekt wie in den Übersichtsgrafiken Abbildung 3 und Abbildung 4 dargestellt in Testelemente aufgeteilt, zu denen konkrete Testfälle auszuführen sind (siehe folgende Seiten).

Die Aufteilung erfolgte dabei

1. der Logik von [BSI TR-03109-1] folgend in

- Testelemente, die Protokolle und Kommunikationsverbindungen laut Kapitel 3 [BSI TR-03109-1] mit Schwerpunkt auf Interoperabilitätsanforderungen (Abbildung 3) und Testelemente, die die Verwendung des SMGW laut Kapitel 4 und 5 [BSI TR-03109-1] mit Schwerpunkt auf funktionale Anforderungen (Abbildung 4)

betreffen.

Die konkret identifizierten Testelemente ergeben sich dann

2. der nächsten Gliederungsebene [BSI TR-03109-1] entsprechend

- als spezifizierte Protokolle und Kommunikationsimplementierungsteile an den Schnittstellen des SMGW, in der TS betrachtet in Kapitel 3 respektive
- als konkrete Anwendungsfälle und im Einsatz zu erfüllende Aufgaben, in der TS betrachtet in Kapitel 4.

Schraffierte Elemente befinden sich zum Zeitpunkt der Erstellung des Testkonzeptes noch in Spezifikation oder Überarbeitung.

Anlage D enthält eine Übersicht aller Testelemente gemäß vorliegendem Konzept und – insofern erforderlich – eine inhaltliche Unterteilung dazu.

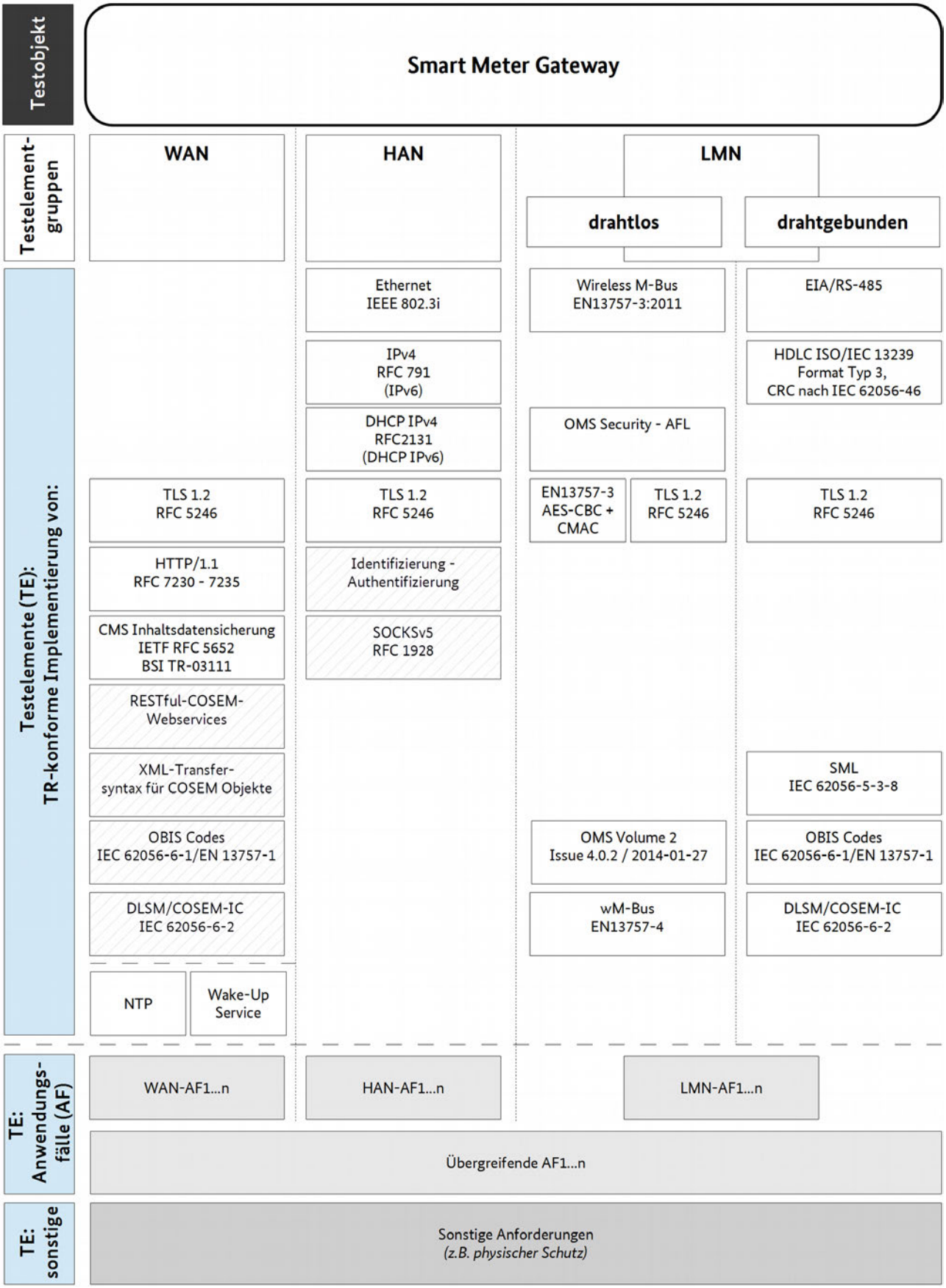

Abbildung 3: Testelemente SMGW (1) – protokollbezogene TE

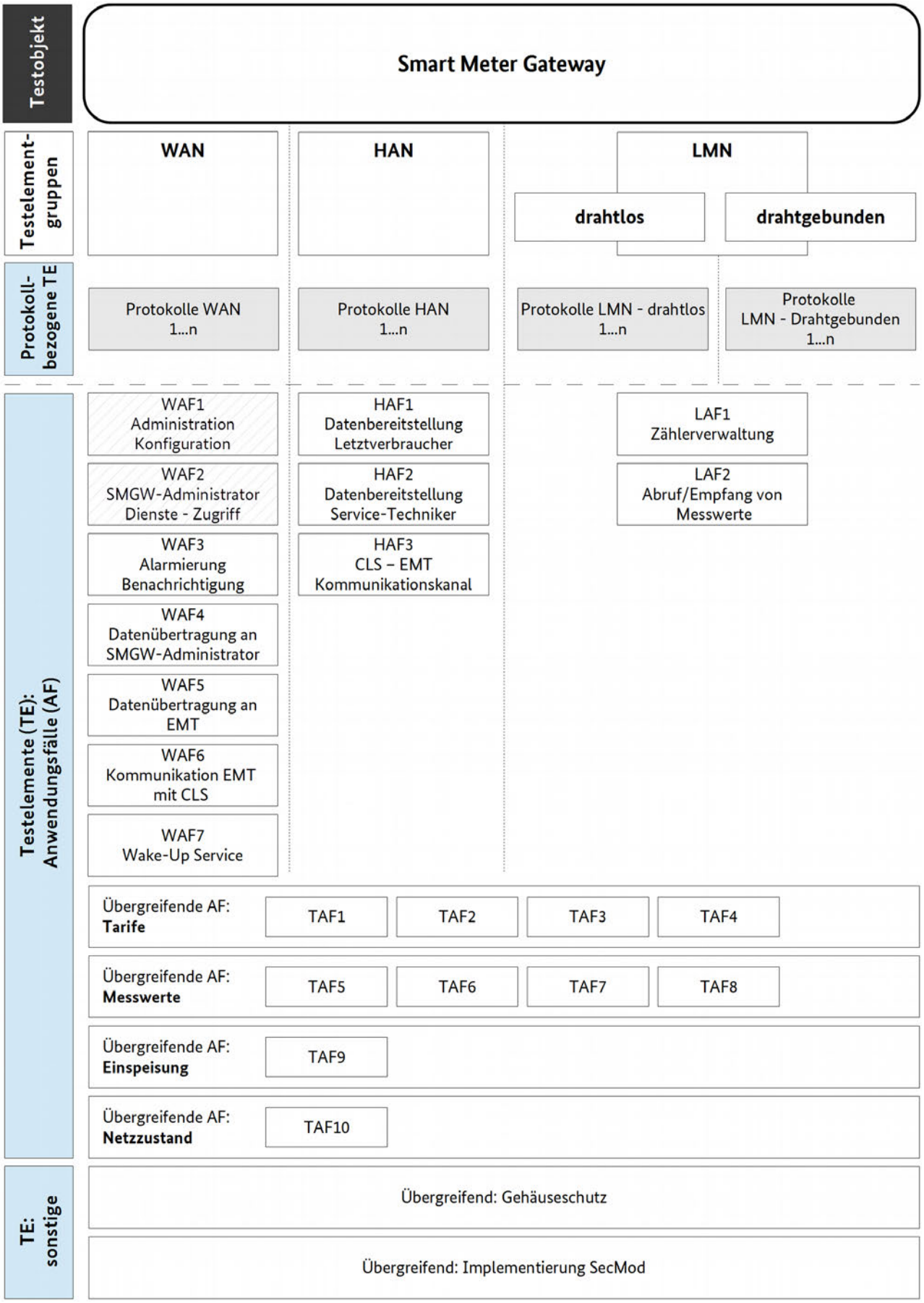

Abbildung 4: Testelemente SMGW (2) – anwendungsfallbezogene TE

2.1.2 Bewertungskriterien für Testelemente

Tabelle 7 - Bewertungskriterien für ein Testelement (Vorlage) - zeigt auf, wie die ermittelten Testelemente initial für die Erstellung der Spezifikation bewertet wurden, um eine Indikation für die Testtiefe zu erhalten. Diese Bewertungstabelle findet sich mit der jeweiligen Bewertung eingangs der testelementspezifischen Abschnitte der Kapitel 3 bzw. 4 im vorliegenden Dokument wieder.

Tabelle 7 enthält in der Spalte „Erläuterung/Hinweise“ auch Erklärungen zum Bewertungsmaß.

Das prinzipielle Vorgehen bei der Bewertung ist – in Reihenfolge – nachstehend beschrieben und beruht auf einer abstrakten, nicht an konkreten Implementierungen orientierten Einschätzung. Diese Bewertung wird im Rahmen der Revision der Bezugsdokumente (vgl. Kapitel 1.3) regelmäßig zu überprüfen und ggf. zu adaptieren sein.

Auf erster, oberster Ebene wird für das Testelement ermittelt:

- Sind in [BSI TR-03109-1] explizite Interoperabilitätsvorgaben für das Testelement definiert?
- Trifft [BSI TR-03109-1] explizit Festlegungen zur Funktionalität für das Testelement?

Auf zweiter Ebene erfolgt eine Bewertung des Testelements anhand folgender Kriterien:

- Beruht das Testelement auf einer ausschließlich durch das Regelwerk [BSI TR-03109] definierten Implementierung?
  Indikation für: Testtiefe und Testintensität (vgl. auch Spalte „Erläuterung/Hinweise“ in Tabelle 7)
- Ist die Anforderung an das Testelement nach Stand der Technik regelmäßig durch die Verwendung integrierter, ggf. bereits geprüfter Bauteile implementiert (z. B.: Netzwerkadapter)?
  Indikation für: Testart (vgl. zu anzuwendenden Testarten auch Kapitel 2.2)
- Welche und wie viele Konfigurationsmöglichkeiten existieren für das Testelement?
  Indikation für: Testermittlungsmethode(n) sowie Testtiefe und Testintensität
- Existieren hinreichend geeignete Testverfahren, um die Anforderung zu überprüfen?
  Indikation für: Testart, generell: Testbarkeit (auch im Hinblick auf vorgegebene Testarten)

Auf dritter Ebene werden projektspezifische Kriterien zur Bewertung hinzugezogen:

- Wie stabil ist die bzw. sind die zugrunde liegenden Anforderungen?
- Kann das Testelement durch die vorgegebenen Testarten / Testverfahren überprüft werden?

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung *hier: Bedeutung für das Konzept*
1	Interoperabilitäts-vorgaben	Gewichtung	A / B / C	Je höher die Bewertung ausfällt, desto mehr Testfälle werden erwartet.
1	Funktionalitäts-vorgaben	Gewichtung	A / B / C	Je höher die Bewertung ausfällt, desto mehr Testfälle werden erwartet.
2	TR-spezifische Anforderung	Auswahl	ja / nein	Handelt es sich um eine spezifisch mit der TR eingeführte Anforderung, sind intensivere Tests erforderlich. Es kann nicht davon ausgegangen werden, dass bereits etablierte (bewährte) Lösungen vorliegen.
2	Implementierung in Hardware	Auswahl	ja / nein	Für direkt – regelmäßig nicht durch den Hersteller des SMGW selbst produzierte – in Hardware implementierte Anforderungen sind weniger intensive Tests vorzusehen.[7]
2	Konfigurations-möglichkeiten	Gewichtung	A / B / C	Je höher die Bewertung ausfällt, desto mehr Testfälle werden erwartet. Für die Ermittlung kann u. U. eine Grenzwertanalyse erforderlich sein.
2	Informativ: bekannte Sicherheitsrisiken und Angriffsszenarien	Auswahl	ja / nein	Bekannte Angriffsszenarien bzw. Sicherheitsrisiken können u. U. zu mehr Testfällen führen (insofern durch die definierten Testarten und innerhalb des gesteckten Anforderungsrahmens möglich) bzw. wären Input für Tests im Rahmen der CC-Evaluierung
2	Testbarkeit mit bekannten Testarten	Auswahl	ja / nein	Sind keine (ausreichenden) Testarten zum Nachweis der Anforderungserfüllung bekannt, muss ein entsprechender Hinweis gegeben werden.

7 Hinweis auf Entwicklungen zum Stand der Technik: Auch in Bezug auf untere Protokollschichten des OSI-Schichtenmodells existieren Ansätze, anstelle von dedizierten (und damit wenig flexiblen) Hardwareumsetzungen weitestmöglich auf Softwareimplementierungen zu setzen (z. B. in der Netzwerktechnik). Ob sich – u. a. durch Verfügbarkeit geeigneter Chipsätze (ASIC) – Verschiebungen ergeben, sollte bei zukünftigen Überarbeitungen der TR und davon abhängiger Dokumente bewertet werden.
In diesem Zusammenhang könnten sich bezüglich des Einsatzes qualifizierter Softwarebibliotheken für Protokollimplementierungen auch Anforderungen in Bezug auf signierte (und geprüfte) Bibliotheksversionen ergeben.

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung *hier: Bedeutung für das Konzept*
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung	A / B / C	Die Gewichtung hat Auswirkung auf die Projektarbeit.
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl	ja / nein	Sind die im Projekt definierten Testarten nicht geeignet, muss ein entsprechender Hinweis gegeben werden.

Tabelle 7: Bewertungskriterien für ein Testelement (Vorlage)

175 Die Gewichtung des Bewertungsmaßstabes erfolgt dreistufig. Die möglichen Stufen sind wie folgt festgelegt:

Bewertungsmaßstab	Erläuterung, Kriterien
A	hoch / viele / umfangreich
B	mittel
C	gering / wenige

Tabelle 8: Legende: Gewichtung für den Bewertungsmaßstab

176 Hinweis: Es ist nicht vorgesehen, die Bewertungsergebnisse aufzusummieren.

Hinweis zur Anforderungsstabilität: eine hohe Anforderungsstabilität bedeutet, dass nach aktuellem Kenntnisstand ein entsprechend hoher Beschreibungsumfang im Konzept / in der Spezifikation erreicht werden kann.

Die Konkretisierung der Testtiefe erfolgt in AP2.

177 2.2 Testverfahren

178 Das Kapitel (2.2) hat informativen Charakter.

179 Es werden die für die Testspezifikation vorgesehenen Testarten kurz beschrieben und deren konkrete
180 Anwendung in den Kapiteln 2.2.1 respektive 2.2.2 erläutert.

181 Zur Prüfung von Komponenten und Systemen stehen eine Reihe von etablierten Testarten und -verfahren
182 zur Verfügung:

183 - statische Tests in Form von
    - 184 Codereviews, die ausgewählte Teile oder den gesamten Sourcecode manuell oder automatisiert
      185 auf Fehler und / oder die Einhaltung von Vorgaben überprüfen,
    - 186 Tests der Dokumentation des Testobjektes, z. B. auf Vollständigkeit oder
    - 187 dokumentationsbasierten Tests, bei denen das Testobjekt dahingehen überprüft wird, ob gefor-
      188 derte Funktionalitäten korrekt beschrieben sind, ohne dass das Testobjekt zur Ausführung
      189 kommt und
190 - dynamische Tests als
    - 191 spezifikationsorientierte Tests, die die Testbedingungen aus der Funktionalität des Testobjektes
      192 herleiten, ohne die programmiertechnische Umsetzung zu berücksichtigen – sog. Black-Box-
      193 Tests und

- strukturorientierte Tests, die sich an der Softwareprogrammierung des Testobjektes ausrichten bzw. diese betrachten – sog. White-Box-Tests.

Der Nachweis, dass ein SMGW zu den Anforderungen der [BSI TR-03109-1] konform ist, soll durch statische Tests der Dokumentation sowie durch dynamische, spezifikationsorientierte Tests, auch Black-Box-Tests genannt, vorzugsweise in Form von automatisierten Funktionstests, erbracht werden.

Die Auswahl ergibt sich aus dem definierten Testinhalt: andere Testverfahren kommen zum einen nicht in Betracht, da sich damit keine Erkenntnisse in Bezug auf die Konformität zu den Anforderungen aus [BSI TR-03109-1] gewinnen lassen bzw. bewusst keine Anforderungen in [BSI TR-03109-1] gestellt werden, die Hersteller von SMGW z. B. hinsichtlich Programmierstandards oder Programmstrukturen der Kommunikationseinheit einhalten müssten. Außerdem soll die Wahl der Testarten auch berücksichtigen, dass eine Testdurchführung in zumutbarer Weise möglich ist und z. B. keine unbilligen Markteintrittsbarrieren[8] geschaffen werden, die dem Aufbau und der Nutzung intelligenter Energiesysteme behindern würden.

Wird mit Bearbeitung der AP2 und ggf. 3 festgestellt, dass eine Anforderung [BSI TR-03109-1] nicht oder nicht in ausreichender Testtiefe mit den vorstehend festgelegten Testverfahren testbar ist, so muss unter Angabe der ermittelten Gründe der Test (u. U. vorerst) in eine Ausschlussliste übernommen werden.

2.2.1 Dokumentationsprüfung

Beim Test der Dokumentation des Testobjektes wird nicht das Testobjekt selbst, sondern nur dessen Dokumentation überprüft. Testfälle zur Dokumentation stellen z. B. sicher, dass die Eingangskriterien für die Ausführung dynamischer Tests erfüllt sind.

Insbesondere wenn die Erfüllung von Anforderungen der [BSI TR-03109-1] über Herstellererklärungen nachgewiesen werden kann, wird dies durch eine Dokumentationsprüfung umzusetzen sein. Hierzu sind im Rahmen der Testfallspezifikation entsprechende Formulare[9] zu erstellen, welche dann durch den Hersteller eines SMGW-Produktes ausgefüllt zur Prüfung zu übergeben sind. Erwartet werden z. B. Angaben

- zu Protokollversionsnummern und ggf. Anlagen und technischen Korrekturen dazu, die implementiert wurden
- zu unterstützten (optionalen) Funktionen und
- zu Grenzwerten / Mengen von unterstützen Funktionen, die für die Implementierung praktisch gesetzt wurden (wenn aus der TR keine direkten Vorgaben ableitbar sind).

8 Eine Synchronisation der Testspezifikation mit ggf. gleichwertigen Regelungen nach europäischem oder sonstigen Recht erfolgt im Rahmen des Projektes ausdrücklich nicht.

9 Ggf. können aus der ITU-T X-Recommendations Serie (Themenbereich der X-Serie: Data networks, open system communications and security), insbesondere X.850 – X.899: OSI applications, Vorgaben direkt übernommen werden. Vgl. u. a. ITU-T X.863 zu Protocol Implementation Conformance Statement (PICS) Proforma. Hyperlink-Hinweis: http://www.itu.int/ITU-T/recommendations/index.aspx?ser=X

2.2.2 Spezifikationsorientierte Tests (Black-Box-Tests)

Die Black-Box-Tests sind

- als Tests mittels Testsuite/Testsuiten, bei denen zu überprüfende Komponenten an ein Testsystem angeschlossen werden, welches die Schnittstellen der anderen an der Kommunikation beteiligten Komponenten simuliert oder
- als Tests zur Integrationsprüfung, bei denen der Prüfgegenstand in ein bestehendes (oder simuliertes) System integriert und seine Reaktion ausgewertet wird,

vorzusehen.

Die Testfälle für die Black-Box-Tests werden ausschließlich systematisch ermittelt. Nach Anforderungslage ist zu entscheiden, ob eine Grenzwertanalyse durchzuführen ist. Dabei spielen ausschließlich fachliche Bewertungskriterien eine Rolle; eine Priorisierung anhand wirtschaftlicher Aspekte erfolgt nicht, da durch die Gesamtheit der spezifizierten Tests eine möglichst vollständige Anforderungskonformität zu [BSI TR-03109-1] nachgewiesenen werden soll. Dies bedeutet auch, dass keine optionalen und auch keine über die TR hinausgehenden Testfälle vorzusehen sind.

Die Testfälle für Black-Box-Tests können automatisiert, teilautomatisiert oder manuell ausgeführt werden und sind so spezifiziert, dass die Wahl einer Ausführungsmethode möglichst nicht schon durch die Testfallbeschreibung begrenzt wird. Die konkrete Ausführungsmethode wird damit grundsätzlich durch die eingesetzten Testwerkzeuge in Verantwortung der prüfenden Stelle bestimmt.

Hinweis: Tests zu einer Reihe von Anforderungen an die Bauweise eines SMGW (vgl. Kapitel 4.5) werden voraussichtlich nur manuell ausführbar sein, d. h., die in den Testfällen spezifizierten Testschritte sind durch Testpersonal selbst auszuführen und geeignet zu dokumentieren.

Eine Prüfung zur Vermeidung von Redundanzen in den Testinhalten und damit verbunden die Prüfung der Abhängigkeiten der Testfälle erfolgt in AP2 und AP3.

2.2.3 Testdurchführungs- und Testergebnisdokumentation

Grundsätzlich sind die Konformitätstests so durchzuführen und zu dokumentieren, dass die Anforderungen der DIN EN ISO/IEC 17025[10] erfüllt werden. Das bedeutet u. a.:

- Die Testdurchführung **muss** vollständig und nachvollziehbar aufgezeichnet werden und
- Testergebnisse **sollen** eine eindeutige Bewertung auf Übereinstimmung bzw. Nichtübereinstimmung mit der überprüften Anforderung ermöglichen. Ist eine eindeutige Ergebnisbewertung nicht möglich, **darf** Konformität **nicht** festgestellt werden.

Die Testdurchführung und die dabei ermittelten Testergebnisse **sollen** vorzugsweise automatisiert aufgezeichnet werden. Sind automatisierte Tests nicht möglich, **müssen** Testdurchführung und Testergebnisse nach einem definierten Verfahren protokolliert werden. Dies ist z. B. mittels entsprechender Formulare und Checklisten möglich.

2.3 Testeingangskriterien für das Testobjekt

Für die Durchführung der Konformitätstests **muss** das Testobjekt u. a. folgende Testfall-unabhängigen Eingangskriterien erfüllen:

- Das Testobjekt ist eindeutig identifizierbar, so dass zweifelsfrei festgestellt werden kann, ob es sich um das korrekte Testobjekt handelt.

10 Es kann auch eine andere Vorschrift gemacht werden, entscheidend ist, dass die prüfende Stelle die benötigte Kompetenz wie beispielsweise in der zitierten Norm beschrieben besitzt.

- Das Testobjekt verfügt über ein Sicherheitsmodul, das nachweislich die Anforderungen der [BSI TR-03109-2] erfüllt.
- Das Testobjekt erfüllt bauartspezifische Zulassungsbedingungen, u. a. um eine gefahrlose Ausführung des Testobjektes im Testlabor zu ermöglichen.
- Das Testobjekt verfügt nachweislich über mindestens eine Implementierung der OSI-Protokollschichten 1- 4 an der WAN-Schnittstelle. Die Implementierung ist hinreichend beschrieben.

2.4 Aufbau eines Testfalls

In diesem Kapitel werden die Einordnung der Testfälle in die Spezifikation und Notation sowie Aufbau der Testfallbeschreibung für die dynamischen Testfälle der TS beschrieben.

Wie in etablierten Frameworks für Konformitätstests ([ISO/IEC 9646-1], [ETSI ETS 300 406] oder [ETSI EG 202 568]) wird ein mehrstufiger Ansatz umgesetzt (vgl. Abb. 5)[11].

Auf Grundlage der Basisspezifikationen [BSI TR-03109-1] werden → Test-Anforderungen ermittelt sowie eine → Testsuite-Struktur und → Test Purposes festgelegt (entspricht etwa dem vorliegenden Konzept-dokument).

Aufbauend darauf werden natürlichsprachliche → Testfälle (Test Cases) in einer XML-Sprache (siehe Anlagen) erstellt. Diese Testfälle sind eine Beschreibung der notwendigen Testschritte auf oberer Ebene (sog. High-level Test Cases), mit deren Hilfe ermittelt wird, ob eine Implementierung den Vorgaben entspricht.

Die XML-Sprache ist so entworfen, dass unabhängig von den zum Einsatz kommenden Testwerkzeugen eine möglichst einfache und robuste Transformation in andere Formate (z. B. für Testfallskelette für eine ausführbare Testimplementierung) möglich ist. Sie ist an High-level Test-Beschreibungssprachen wie etwa TPLan [ETSI ES 202 553] angelehnt – mit weniger Formalität bei der Beschreibung von Testdaten und Testverhalten. Die Summe aller erstellten Testfälle ergibt die → abstrakte Testsuite.

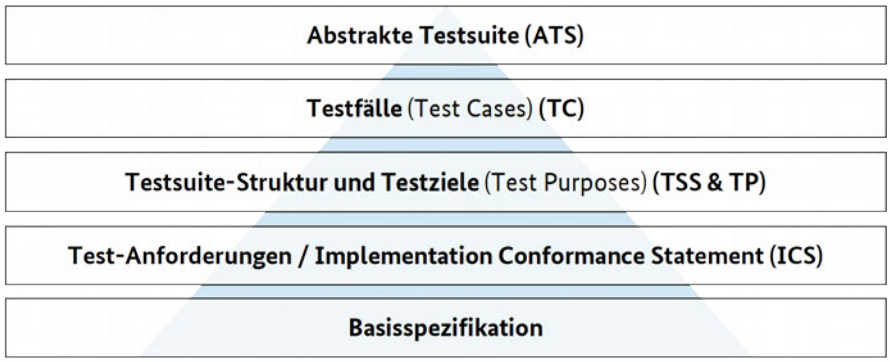

Abbildung 5: Einordnung der Testfälle in die Testspezifikation (Vorgehensmodell)

Es ist nicht Ziel der [BSI TR-03109-TS-1], direkt ausführbare Testfälle abzubilden. Daher wird in der Beschreibung keine Programmiersprache wie Java oder Python benutzt. Die abstrakte Testsuite ist textuell und das Testverhalten sowie die Testdaten sind beschrieben, ohne plattformabhängig und ausführbar zu sein. Die Testsuite bleibt so frei adaptierbar für die unterschiedlichen Bedarfe von Prüflaboren und Test-objekten.

Bei der Beschreibung der einzelnen Testfälle sind die folgenden Eigenschaften anzugeben:

11 Da die referenzierten Standards in englischer Sprache vorliegen – und regelmäßig zum Einsatz kommen – wird darauf verzichtet, in der Konzeption eine eigene Übersetzung einzuführen.

Eigenschaft	Beschreibung
ID	eine eindeutige fortlaufende Nummer zur Identifikation des Testfalls
Name	die eindeutige Bezeichnung eines Testfalls; gibt durch den Aufbau einen Hinweis auf die Zugehörigkeit des Testfalls zu einer Testfallgruppe oder einer Testsuite
Version	die Version des Testfalls
Anforderungen	die Anforderungen, auf die sich der Testfall bezieht
Verschlüsselung	die im Test verwendete Verschlüsselung
Schnittstellen	die an der Testdurchführung beteiligten Schnittstellen
Testkonfiguration	die Festlegung, welche Interfaces die Points of Control and Observation sowie das System Under Test (SUT) darstellen
Protokollebene	die Schichten nach OSI-Referenzmodell, die getestet werden
Testdaten (Test Data)	die natürlichsprachlich beschriebenen Testdaten, die mit den einzelnen Testschritten verknüpft sind
Testfalltyp	die Art des Testfalls[12]
Hinweise	Hinweise zur Durchführung des Testfalls.
Beschreibung	Eine Beschreibung, was mit dem Test geprüft wird.
Vorbedingungen	Bedingungen, die Voraussetzungen für die Durchführung des Testfalls sind.
Testschritte	Die durchzuführenden Testschritte.
Erwartete Ergebnisse	Die in den Testschritten zu erwartenden Ergebnisse.
Rollback-Operation	Wenn vorhanden der Testfall, mit dem die Aktionen rückgängig gemacht werden können und das SMGW so in den Ausgangszustand versetzt werden kann.

Tabelle 9: Angaben zu einem Testfall

Die Beschreibung der Testdaten erfolgt strukturiert und konkret für die Testfälle. Die Struktur kann testelementspezifische Ausprägungen haben und wird innerhalb des nachstehend beschriebenen XML-Gerüstes in `testdata.xml` durch geeignete HTML-Elemente abgebildet. Damit wird eine separate Testdatenhaltung wie in der Beschreibung der Testinfrastrukturanforderungen (Kapitel 2.6) gezeigt, unterstützt.

Sind für Testfälle Wertebereiche zulässig, so werden lediglich diese Bereiche angegeben. Grenzwerte und Einzelwerte sind stets konkret vorgegeben[13] bzw., insofern es sich um Ergebnisse der Ausführung von als Vorbedingung formulierten Testfällen handelt, mit entsprechender Referenzierung auf den datenerzeugenden Testfall dargestellt (das erwartete Ergebnis des datenerzeugenden Testfalles ist dann ebenso entsprechend der Testdatenstrukturvorgaben formuliert).

Der Aufbau der abgeleiteten XML-Struktur wird anhand der abgebildeten, beispielhaft befüllten Testsuite-Darstellung (Abbildung 6) deutlich. Einen schematischen Überblick gibt Abbildung 7.

12 Laut Projektauftrag sind je nach Anforderung Positiv- und Negativtestfälle vorzusehen. Ergänzend zur Terminologie nach [ISTQB®-Glossar] bedeutet dies, dass zwischen Testfällen unterschieden werden soll, die ein spezifikationskonformes Verhalten des Testobjektes sowohl bei Tests
a) mit spezifikationskonform formulierten Testvorbedingungen (Positivtestfall) als auch
b) mit außerhalb der Spezifikation formulierten Testvorbedingungen (Negativtestfall) erwarten.

13 Dies setzt voraus, dass die Bezugsdokumentation die Herleitung konkreter Testdaten zulässt. Existieren für Testelemente keine konkreten Vorgaben bzw. sind die Bezugsdokumente noch nicht final, ist auf eine abstrakte Testdatenbeschreibung zurückzugreifen.

```xml
<?xml version="1.0" encoding="UTF-8"?>

<testsuite xmlns="http://bsi.bund.de/tr-03109-1"
  xsi:schemaLocation="http://bsi.bund.de/tr-03109-1 bsi_tr-03109-1.xsd"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:html="http://www.w3.org/1999/xhtml"
  xmlns:xi="http://www.w3.org/2001/XInclude">

  <xi:include href="interfaces.xml"/>
  <xi:include href="testconfigurations.xml"/>
  <xi:include href="testdata.xml"/>
  <xi:include href="preconditions.xml"/>

  <testcases>
    <xi:include href="testcase.xml"/>
    <xi:include href="wake_up.xml"/>
    <xi:include href="testcase_TLS_Handshake.xml"/>

    <derived-testcase id="51" name="Wake-Up Service TF Variante" parentid="49">
      <testdatasets>
        <testdata name="wake-up-paket" ref="wake-up-tls-paket"/>
      </testdatasets>

      <preconditionsref name="preconditions1"/>

    </derived-testcase>
  </testcases>

</testsuite>
```

Abbildung 6: Beispiel: Testsuite in XML-Notation (main.xml)

297 Hinweis: Der Verweis auf die jeweilige Anlage ist in den grün hinterlegten Boxen der folgenden Abbildung
298 wiedergegeben.

299 Die Anlagen enthalten die konkreten Vorgaben für die XML-Daten.

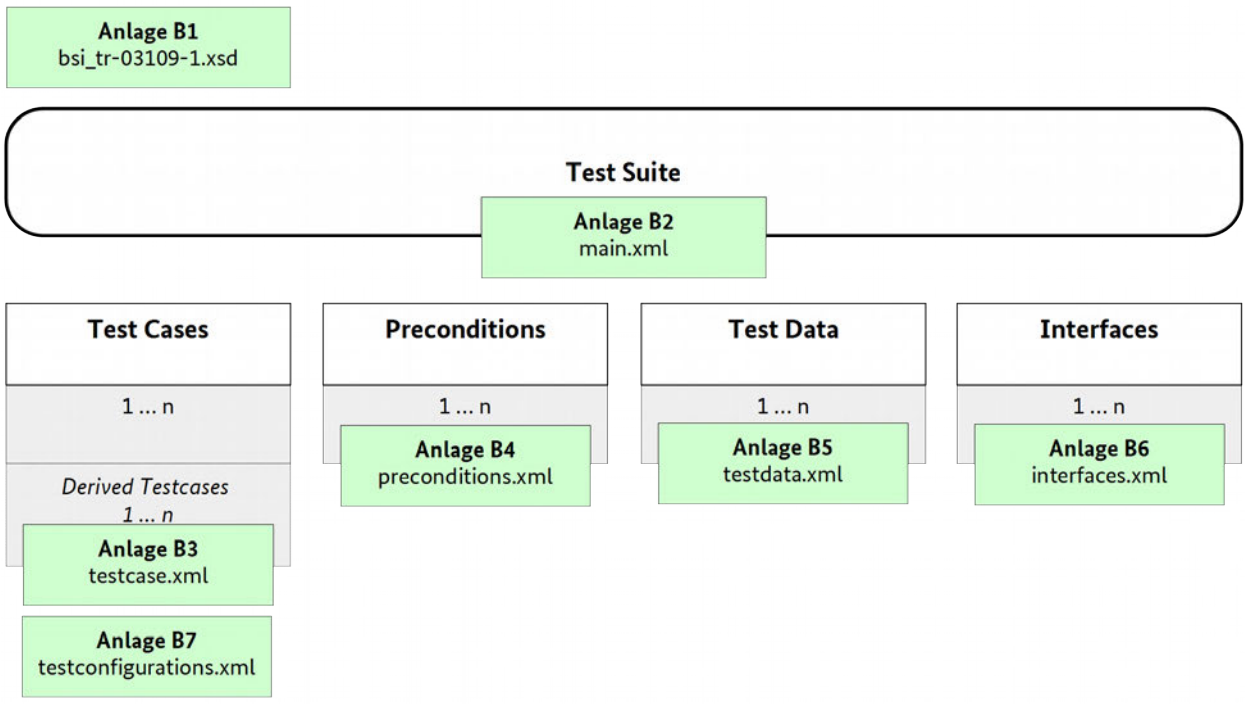

Abbildung 7: Struktur XML-Dateien (mit Referenz auf Anlagen)

Anlage	Erläuterung
B1	XML-Schemabeschreibung
B2	Testsuite – Zusammengesetzt aus – 1 ... n Beschreibung(en) der Schnittstellen (`interfaces.xml`) – 1 ... n Beschreibung(en) der Testdaten (`testdata.xml`) – 1 ... n Beschreibung(en) der Vorbedingungen (`preconditions.xml`) – 1 ... n Beschreibung(en) der Testfälle
B4	Vorbedingungen – zusammengesetzt aus – 1 ... 1 Beschreibung der Vorbedingung – 0 ... 1 Testfall-ID (Test Case ID)
B3	Testfälle 1 ... n Testfälle (Test Cases), abgeleitete Testfälle (Derived Test Cases)

Tabelle 10: Aufbau der XML-Struktur - Teil 1 - allgemein

300 Ein Testfall enthält die Angaben laut Tabelle 9 und setzt sich wie folgt zusammen:

Anlage	Erläuterung
B5	0 ... n Testdaten-Beschreibungen
B7	1 ... 1 Testkonfigurationsbeschreibung mit folgenden Angaben – 1 ... 1 Beschreibung zur Verschlüsselung – 1 ... 1 Beschreibung zum verwendeten Testtreiber/Stub der höher liegenden OSI-Schicht (Upper Tester Interface) – 1 ... 1 Beschreibung zum verwendeten Testtreiber/Stub der niedriger liegenden OSI-Schicht (Lower Tester Interface) – 1 ... 1 Beschreibung zur betrachteten logischen Schnittstelle des Testobjektes (SUT) (Anlage B6: `interfaces.xml`)

Tabelle 11: Aufbau der XML-Struktur - Teil 2 - Testfälle

301 Zwei Beispiele für die konkrete Formulierung von Testfällen finden sich in Anlage A.

302 Die Metadaten können um weitere Informationen angereichert werden:

303 • So kann in den Testfällen ein dediziertes Feld aufgenommen werden, welches eine Aussage darüber
304 trifft, ob der Testfall eine Nutzung des SecMod bei der Ausführung der Testschritte erwartet. Eine
305 konkrete Feststellung, ob das SecMod tatsächlich verwendet wird, kann durch die spezifizierten Testfälle
306 jedoch nicht getroffen werden.

307 • Die Points of Control and Observation (vgl. Kapitel 2.6) können explizit aufgeführt werden.

308 • Prüfauftragsspezifische Informationen der testausführenden Entität können mit geführt werden.

309 2.5 Testabgrenzung

310 Die Konformitätstests nach vorliegender TS beziehen sich ausschließlich auf den Nachweis der Erfüllung
311 von Anforderungen aus [BSI TR-03109-1].[14] Konformität zu [BSI TR-03109-1] bedeutet also hier, dass eine

14 Vgl. gegensätzliche Auffassung in [**TSE-TA**], Kapitel 1 (u. a. 1.1).

SMGW-Implementierung unter Laborbedingungen Funktionalitäts- und Interoperabilitätsanforderungen im Geltungsbereich der [BSI TR-03109] umsetzt.

Die Tests sind jedoch allein **kein** Nachweis hinsichtlich der allgemeinen Qualität eines SMGW, insbesondere nicht für Qualitätsmerkmale, zu denen keine Anforderungen in [BSI TR-03109-1] aufgestellt werden und dementsprechend z. B. kein Nachweis über die Sicherheit eines konkreten SMGW-Produktes.

Die Tests erfolgen unter Laborbedingungen[15] und haben nicht zum Ziel, Interoperabilität mit konkreten existierenden und zukünftigen Produkten im geplanten Einsatzumfeld von Smart Meter Gateways nachzuweisen.

Es ist sowohl in Abhängigkeit zum aktuellen Stand der Technik als auch in Abhängigkeit zu der konkreten Produktumsetzung für ein SMGW zu evaluieren und zu entscheiden, welche sicherheitsbezogenen und sonstigen Prüfungen zusätzlich zu den in [BSI TR-03109-TS-1] spezifizierten Tests erforderlich sind. Z. B. können sich aus einer konkreten Produktumsetzung Interoperabilitätsaspekte oder Angriffsszenarien ergeben, die im Rahmen der hier spezifizierten Konformitätstestfälle nicht durch [BSI TR-03109-TS-1] oder [GW_PP] vorhersehbar bzw. mit geeigneten Testfällen (präventiv) abdeckbar sind.

Anforderungen des Schutzprofils für das SMGW (vgl. [GW_PP]), welche als Vorbedingung[16] für die Anforderungserfüllung nach [BSI TR-03109-1] gelten können, sind im Rahmen der CC-Evaluierung zu überprüfen[17]. Es ist davon auszugehen, dass eine Konformität zu [BSI TR-03109-1] nicht erreicht werden kann, wenn die CC-Evaluierung negativ ausfällt.

Konformitätsanforderungen, die ein SMGW-Produkt aufgrund seiner Bauart allgemein (z. B. elektromagnetische Verträglichkeit) oder aufgrund herstellerseitig gewählter Schnittstellenimplementierungen (z. B. in Bezug auf Vorgaben für Funkanlagen und Telekommunikation) erfüllen muss, werden nicht durch die Testspezifikation geprüft, sondern sind ggf. als Testeingangskriterien für das Testobjekt nachzuweisen.

Die Abgrenzung der Testinhalte bezogen auf die zu untersuchenden Systemmerkmale wird unter Anwendung der Definitionen für Systemqualitätsmerkmale nach ISO/IEC 25010:2011 vorgenommen (vgl. dazu auch Kapitel 1.4)[18]. Abbildung 8 zeigt eine Übersicht der Qualitätsmerkmale, auf die ein IT-System nach ISO/IEC 25010:2011 untersucht werden kann. Für [BSI TR-03109-TS-1] als relevant definiert sind die Merkmale Funktionalität und Interoperabilität (in der Abbildung rot markiert). Die Sicherheitsaspekte sind Gegenstand der CC-Evaluierung nach [GW_PP].

15 Standardisierte Testtreiber und ggf. der Aufbau einer Referenztestumgebung, die alle (wesentlichen) Produktimplementierungen, mit denen ein SMGW interoperabel sein soll, enthält, können in Bezug auf ein konkretes Testobjekt der [BSI TR-03109-TS-1] die Aussagekraft hinsichtlich der Interoperabilität im Feldeinsatz weiter unterstützen. Grundsätzlich kann ein „Feldtest“ jedoch nicht allein durch einen Labortest ersetzt werden.

16 Die Konkretisierung für [BSI TR-03109-TS-1] erfolgt testfallspezifisch.

17 Liegen zu Beginn des Tests nach [BSI TR-03109-TS-1] (noch) keine Nachweise dazu vor, sind ggf. entsprechende Erklärungen abzugeben. Werden diese Erklärungen im Verlauf der CC-Evaluierung nicht bestätigt, kann auch keine Konformität zu [BSI TR-03109-1] erreicht werden. Es muss darauf geachtet werden, dass die Prüfgegenstände/Testobjekte aus CC-Evaluierung und Konformitätstest übereinstimmen. Dies ist organisatorisch zu regeln und nicht Gegenstand der TS.
Etwaige Abhängigkeiten zwischen den Anforderungen CC und den Konformitätsanforderungen sind herstellerseitig zu berücksichtigen.

18 Das Testobjekt wird für die vorliegende Konzeption als IT-System angesehen.

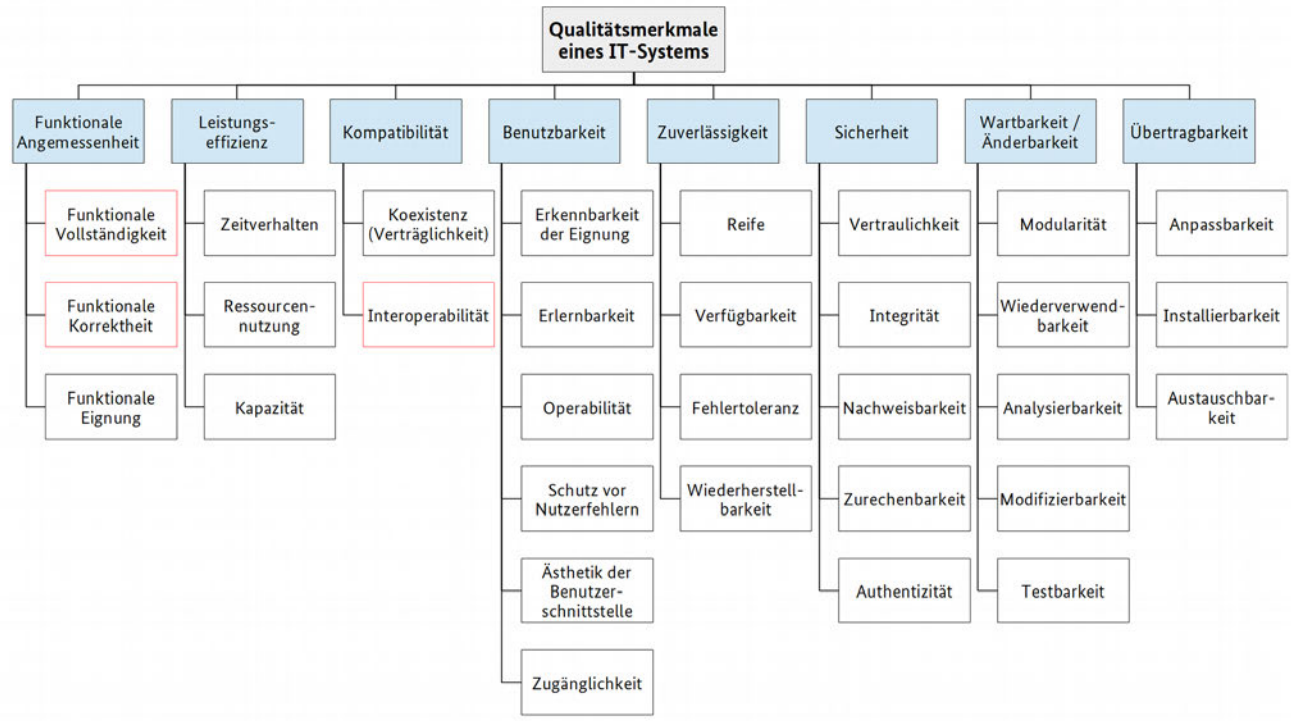

Abbildung 8: Qualitätsmerkmale nach ISO/IEC 25010:2011

342 Ausnahmsweise in die Konformitätsbewertung aufgenommen werden Tests zu anderen Merkmalen nur
343 dann, wenn hierzu in [BSI TR-03109-1] eine Anforderung ausdrücklich und konkret formuliert ist.

Anforderungen, die nach aktuellem Kenntnisstand nicht oder nur eingeschränkt testbar sind, werden in Anlage C aufgelistet.

344 Abgrenzung Testabdeckung für [BSI TR-03109-TS-1]: Interoperabilität

345 Tabelle 12 gibt einen Überblick zu den aus [BSI TR-03109-1] herleitbaren Interoperabilitätsaspekten, die an
346 den definierten logischen Schnittstellen auf Anforderungskonformität geprüft werden können. „Explizit“
347 bedeutet, dass zu den in der TR definierten Anforderungen konkrete Testfälle vorgesehen sind, die die
348 Anforderungserfüllung bestätigen sollen.[19]

19 An dieser Stelle wird keine Aussage über technische Machbarkeit der Testfälle getroffen.

Logische Schnittstelle	Anbindung	Verbindung	Syntax	Semantik
WAN	Kein Testgegenstand	Ab Transport-sicherungsschicht	Explizit (COSEM-Webservices)	Implizit (Explizit Gegenstand der Funktionstests zu den Anwendungs-fällen)
HAN: IF_GW_CLS	Beschränkt auf das vorgeschriebene Ethernet-Interface	Beschränkt auf den Internet-Protokoll-Stack	Implizit (Explizit Gegenstand der Funktionstests zu den Anwendungsfällen)	
HAN: IF_GW_CON				
HAN: IF_GW_SRV				
LMN/ drahtlos	Explizit (wM-Bus)	Explizit	Explizit	
LMN/ drahtgebunden	Explizit (EIA/RS-485)	Explizit	Explizit	

Tabelle 12: Mögliche Testabdeckung Interoperabilität an den logischen Schnittstellen

Abgrenzung Testabdeckung für [BSI TR-03109-TS-1]: Funktionalität

[BSI TR-03109-TS-1] spezifiziert ausschließlich Testfälle für Anforderungen aus [BSI TR-03109-1], die durch das definierte Testobjekt erfüllt werden müssen. Funktionale Aspekte, die durch Testobjekt-externe Implementierungen umgesetzt werden müssen, sind nicht Teil der Testspezifikation. Dies betrifft z. B. Anforderungen, die von an den logischen Schnittstellen mit dem SMGW interagierenden Systemen zu erfüllen sind.

Beschreibt [BSI TR-03109-1] Funktionen, für die keine oder keine vollständigen Kommunikationsszenarien vorgegeben sind, um sie zu nutzen oder die nur mit interagierenden Systemen gemeinsam vollständig ausgeführt werden können, ist die Testabdeckung auf diejenigen Funktionsteile beschränkt, die ohne beteiligte Systeme direkt an den logischen Schnittstellen des SMGW aufruf- und testbar sind.

Hinweis: Der in [BSI TR-03109-1] verwendete Begriff „nicht-funktionale Anforderungen“ verwendet nicht den Bezugsrahmen IT-System. Die dort gestellten Anforderungen werden nicht nach den eingangs von Kapitel 2.5 beschriebenen Merkmalen betrachtet.

2.6 Testinfrastruktur, Testumgebung

Dieses Kapitel (2.6) hat informativen Charakter.

Nachfolgend wird eine abstrakte Beschreibung des sich aus den Testfällen der TS ableitenden Testaufbaus gegeben und logische Komponenten benannt. Es wird keine konkrete Testinfrastruktur vorgegeben.

2.6.1 Aufgaben und Aufbau der Testinfrastruktur

Für die Testdurchführung muss die Testumgebung die beteiligten Systeme simulieren.[20]

Zu diesem Zweck werden Testkonfigurationen bzw. die Testarchitektur nach [ISO/IEC 9646-1] angegeben. Es wird hier zwischen IUT (Implementation Under Test), Lower Tester, Upper Tester, Points of Control and Observation (PCO) unterschieden:

20 Es ist denkbar, für den Aufbau einer Testumgebung auf vorhandene Frameworks zur Unterstützung zurückzugreifen. Diese müssen für die Verwendung in der Testumgebung entsprechend den Vorgaben für den Einsatz in einem Prüflabor qualifiziert und ggf. erweitert werden. Vorzugsweise sollen dabei quelloffene Lösungen Verwendung finden oder es wird ein verbindliches Framework entwickelt und allgemein verwendet; Beispiele für existierende, ggf. verwendbare oder weiter entwickelbare Frameworks sind: OpenMUC des Fraunhofer-Instituts für Solare Energiesysteme (http://www.openmuc.org) oder OGEMA-Framework der Open Gateway Energy Management Alliance (http://www.ogema.org).

Implementation Under Test (IUT):

Die Implementierung, die das Testelement darstellt.

System Under Test (SUT):

Das konkrete System, in dem sich die IUT befindet bzw. betrieben wird.

Lower Tester:

Kontrolliert und observiert das sog. „Lower Service Boundary“ des IUT, d. h. es wird nicht direkt an einer IUT Schnittstelle getestet (bzw. das PCO sitzt direkt an der IUT), sondern indirekt über eine Serviceschicht, welche die IUT einbindet.

Upper Tester:

Kontrolliert und observiert die sog. „Upper Service Boundary“ des IUT, d. h. das PCO sitzt direkt an einer IUT Schnittstelle, z. B. über eine API, ein Hardware-Interface oder ähnliches.

Hinweis: Die Granularität der Testfälle (Anzahl der Testschritte) wird auch dadurch bestimmt, dass in einem Testfall kein Wechsel der Tester erfolgen darf.

Point of Control and Observation (PCO):

Ein PCO bildet einen Service Access Point im OSI-Referenzmodell ab: das sind die Schnittstellen, über welche die Tests getrieben werden (Testtreiber) und über welche die Auswertung des erwarteten Testverhaltens erfolgt.

Abbildung 9 gibt schematisch wieder, welche logischen Komponenten und testprozessunterstützenden Funktionalitäten die Testinfrastruktur laut Tabelle 13 und Tabelle 14 zur Verfügung stellen muss. Ein oder mehrere Simulatoren werden benötigt, um das Testobjekt auf der jeweils betrachteten Serviceschicht in der Testumgebung anzusteuern und auf Aktionen des Testobjektes zu reagieren. Diese Simulatoren müssen selbst sowohl konform zu [BSI TR-03109-1] implementiert sein als auch für das Testen von Negativtestfällen kontrollierbar und gezielt nicht-konform agieren können. Je nach Testelement muss ein Simulator eine oder mehrere OSI-Schichten verfügbar machen und diese dem Testobjekt als Upper und/oder Lower Tester an den vorhandenen Schnittstellen bereitstellen. Darüber hinaus müssen die für die Testfälle erforderlichen PCO vorhanden sein.

Während der Lower Tester regelmäßig auf Anwendungsschicht agieren wird, muss der Upper Tester grundsätzlich auf allen OSI-Schichten agieren können und PCO entsprechend bereitstellen. Dies wird auch im Beispiel (Abbildung 9) deutlich.

Die TS stellt der Testinfrastruktur Informationen in Form von XML-Daten wie in Kapitel 2.4 beschrieben zur Verfügung, um Tests zur Ausführung zu bringen. Soweit möglich, werden im Konzept auch Hinweise zu Testwerkzeugen gegeben. Aufgabe der Testinfrastruktur wird es auch sein, die bereit gestellten Test-Informationen (Testdaten, Testkonfigurationen, Vorbedingungen, Testfälle) zu verwalten und zur (automatisierten) Ausführung aufzubereiten.

Hinweis zur Darstellung in Abbildung 9: die für den Test verfügbaren Schnittstellen des SMGW werden technisch mindestens einmal vorhanden sein und die Testumgebung muss die entsprechende Anbindung von Upper und Lower Tester gewährleisten. Aus der Abbildung darf nicht geschlossen werden, dass stets zwei Ein-/Ausgänge pro Schnittstelle am SMGW verfügbar sind.

Komponente	Art	Erläuterung	Vorgaben laut TS
(Test-) SM-PKI	physisch	stellt notwendige Zertifikatsinfrastruktur bereit	`preconditions.xml`
Datenspeicher (DB) Testdaten	physisch	stellt notwendige Testdaten bereit; bereitet konkrete Testdaten auf	`testdata.xml`

Komponente	Art	Erläuterung	Vorgaben laut TS
Datenspeicher (DB) Testkonfigurationen	physisch	hält die Testkonfigurationen vor	`testconfigurations.xml`
Datenspeicher (DB) Messwerte	physisch	speichert die an den PCO aufgenommenen Messwerte und Ist-Testergebnisse, die gegen die in den Testfällen vorgegebenen erwarteten Ergebnisse abzugleichen sind	`testcase.xml`
Upper Tester: Serviceschicht-Simulator	logisch	stellt anforderungskonform die laut TS für einen Testfall erforderlichen Dienste an den SMGW-Schnittstellen zur Verfügung; verfügt über PCO, um den Testablauf zu steuern und die laut Testfall vorgegebenen Ergebnisse zu messen	`testconfigurations.xml` `interfaces.xml` `testcase.xml`
Upper Tester / Lower Tester: EMT-Simulator		siehe Upper Tester: Serviceschicht-Simulator; füllt die in [BSI TR-03109-1] definierte Rolle EMT aus	
Upper Tester / Lower Tester: CLS-Simulator		siehe Upper Tester: Serviceschicht-Simulator; agiert wie ein in [BSI TR-03109-1] definiertes CLS	
Upper Tester / Lower Tester: Zähler-Simulator (in Ausprägungen drahtlos und drahtgebunden)		siehe Upper Tester: Serviceschicht-Simulator; stellt die notwendigen Zählerfunktionen bereit	
Upper Tester / Lower Tester: Letztverbraucher-Simulator		siehe Upper Tester: Serviceschicht-Simulator; füllt die in [BSI TR-03109-1] definierte Rolle Letztverbraucher aus	
XML-Interpreter	physisch	stellt die in XML spezifizierte Testsuite dar / zeigt diese an	`bsi_tr-03109-1.xsd` `main.xml`

Tabelle 13: Komponenten der Testinfrastruktur

Komponente	Art	Erläuterung	Vorgaben laut TS
XML-zu-Testskript-Transformator	optional, physisch	übersetzt die XML-Daten der TS in maschinenausführbare Testskripte; wird nicht von der TS vorgegeben	–
Teststeuerer	optional, logisch	Werkzeug zum Ausführen der in Testskripts übersetzten Testfälle; kann Teil der Simulatoren sein oder diese integrieren; wird nicht von der TS vorgegeben	–

Tabelle 14: Optionale Komponenten der Testinfrastruktur

Für die logische Komponente „Letztverbraucher-Simulator“, über die die Dateneinsichtnahme für die Rolle des Letztverbrauchers zu realisieren ist, wird angenommen, dass die in der TR beschriebene „Anzeigefunktion“ über in der TR vorgegebene Schnittstellen auch abrufbar sein wird.

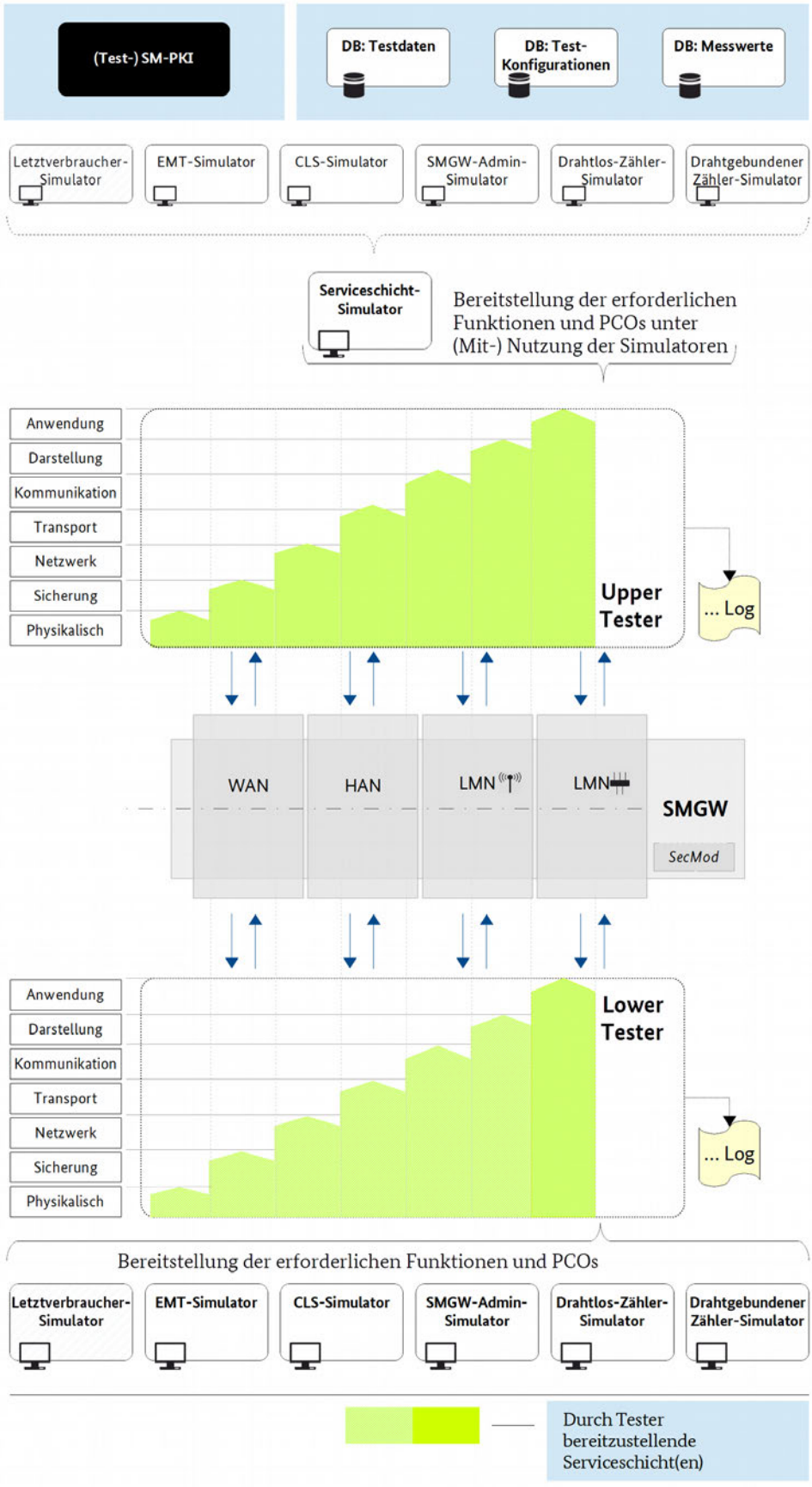

Abbildung 9: Anforderungen an die Testinfrastruktur: Bereitzustellende Dienste / Funktionen

Abbildung 10 gibt einen schematischen Überblick über die abstrakte Testanordnung und zeigt beispielhaft (rote Eintragungen) eine Konkretisierung des Testaufbaus (vgl. Abbildung 9) für einen Test des Kommunikationsszenarios *HKS3: Initierung eines transparenten Kanals durch ein Controllable Local System (CLS)* – ausschnittsweise beschränkt bis zur Kanalaufbau-Anfrage beim externen Marktteilnehmer. Die Schnittstellen des SMGW sind dabei auch hier nur aus Darstellungsgründen mit zwei Ein- Ausgängen eingezeichnet, um die Aufgaben des Lower und Upper Tester zu verdeutlichen.

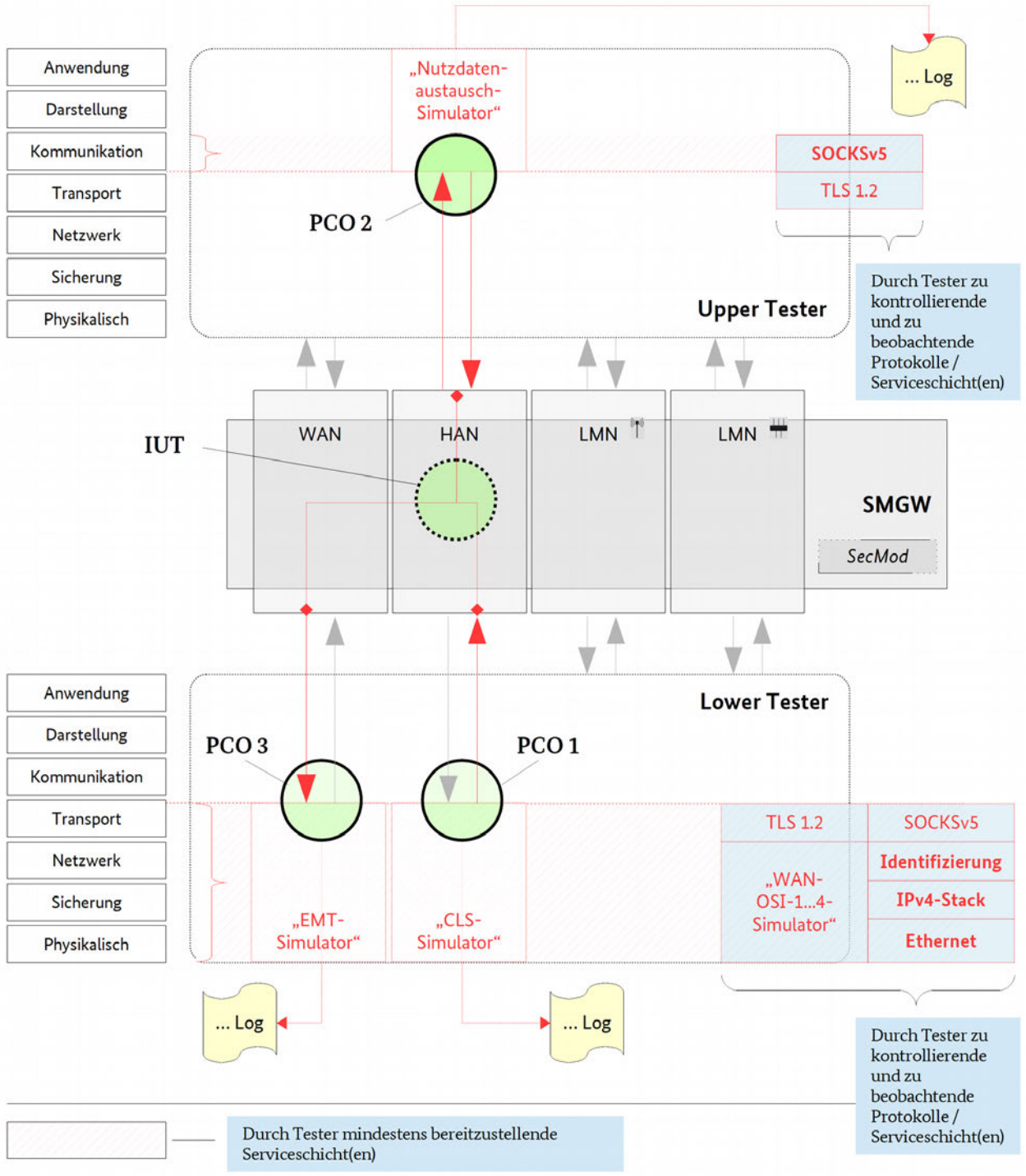

Abbildung 10: Aufbau der Testumgebung (SUT, IUT, Tester) mit Beispiel für Ausschnitt aus HKS3

421 **Erläuterungen zum Beispiel**

422 Die zu untersuchende Implementierung im SMGW (IUT) ist hier die Funktion zur Herstellung eines
423 (transparenten) Kommunikationskanals zwischen externen Systemen unter Nutzung von SOCKSv5 und
424 TLS 1.2 gemäß [BSI TR-03109-1], Kapitel 3.4.3.3.

Lower Tester	Erläuterung
„CLS-Simulator“	Teil der Testumgebung; verfügt über TR-konforme Ethernet, IPv4-Stack-, TLS-1.2- und SOCKS-Implementierungen und kann Identifizierungs- und Authentifizierungsfunktionen eines CLS TR-konform gegen das SUT ausführen; Fungiert als sog. Testtreiber;
„EMT-Simulator“	Teil der Testumgebung; verfügt über eine TR-konforme TLS-1.2-Implementierung und kann die notwendigen OSI-Schichten 1 bis 4 derart bereitstellen, dass die TLS-1.2-Implementierung benutzt werden kann.

Tabelle 15: Erläuterung zu Abbildung 10: Lower Tester

425

Upper Tester	Erläuterung
„Nutzdaten-austausch-Simulator“	Teil der Testumgebung (zu interpretieren als Teil der logischen Komponente „Serviceschicht-Simulator“, vgl. Tabelle 13); wird in einer realen Testumgebung als logische Entität anzusehen sein, welche ab der SOCKS- respektive TLS-Implementierung Fähigkeiten eines CLS- und eines EMT-Simulators benutzt und die Konkretisierung des „Serviceschicht-Simulators“ in Abbildung 9 darstellt; verfügt über TR-konforme TLS-1.2- und SOCKSv5-Implementierung und kann die Aktionen/Reaktionen von CLS und EMT gemäß [BSI TR-03109-1], Kapitel 3.4.3.3, abbilden, z. B. Mitteilung Zieladresse EMT, Simulation dieser Zieladresse, Simulation von Datentransport; fungiert im Testverlauf sowohl als Testtreiber als auch als Teststub

Tabelle 16: Erläuterung zu Abbildung 10: Upper Tester

426

Points of Control and Observation	Erläuterung
PCO 1	Kontrolliert das den Verbindungsaufbau anstoßende, durch die Testumgebung zu simulierende CLS (SOCKS: connect ...); Ist durch den „CLS-Simulator“ bereitzustellen
PCO 2	Kontrolliert die im SMGW stattfindenden Aktionen (`SOCKS-accept, TLS-Handshake, Connect EMT`, ...); Beobachtet die Implementierung im SMGW an den Schnittstellen HAN und WAN; Ist durch den „Nutzdatenaustausch-Simulator“ bereitzustellen
PCO 3	Kontrolliert das Zustandekommen des transparenten Kanals (TLS-Verbindungsanfrage SMGW-EMT wird gestellt); Beobachtet die Implementierung im SMGW; Ist durch den „EMT-Simulator“ bereitzustellen

Tabelle 17: Erläuterung zu Abbildung 10: Points of Control and Observation

Die Anforderungen, die sich aus [BSI TR-03109-1] an Testtreiber und Testkonfiguration ergeben, werden auf Testelementebene benannt und erforderlichenfalls auf Testfallebene konkretisiert. Diese Anforderungen müssen durch die Testumgebung in geeigneter Weise erfüllt werden.

2.6.2 Nutzungsszenarien in der Testumgebung

Die Testumgebung wird benutzt, um die später beschriebenen Testfälle auszuführen. Dazu besteht die Testumgebung aus verschiedenen Komponenten, die allgemein auch einer der folgenden Kategorien zugeordnet werden können:

Testmodul (Upper Tester): Aufgabe eines Testmoduls ist, die Testfälle eines konkreten Testszenarios durchzuführen bzw. dem Tester die Durchführung zu ermöglichen. Dazu verwendet das Testmodul ein Unterstützungsmodul aus der darunterliegenden OSI-Schicht.

Unterstützungsmodul (Lower Tester): Ein Unterstützungsmodul implementiert die Dienste einer bestimmten OSI-Schicht und stellt sie einem Modul der darüber liegenden Schicht zur Verfügung. Beispiele für Unterstützungsmodule wären etwa eine Bibliothek, die den Aufbau einer TLS-Sitzung ermöglicht, oder ein REST-Modul, welches die Schema-valide und Schema-invalide Kommunikation zwischen SMGW und EMT/Administrator ermöglicht.

Für die meisten erforderlichen Protokolle (bspw. HDLC, TLS, NTP) kann davon ausgegangen werden, das schon funktionierende Komponenten verfügbar sind, die genutzt werden können, aber nicht (ohne Weiteres) geeignet sind, um direkt Testfälle auszuführen.

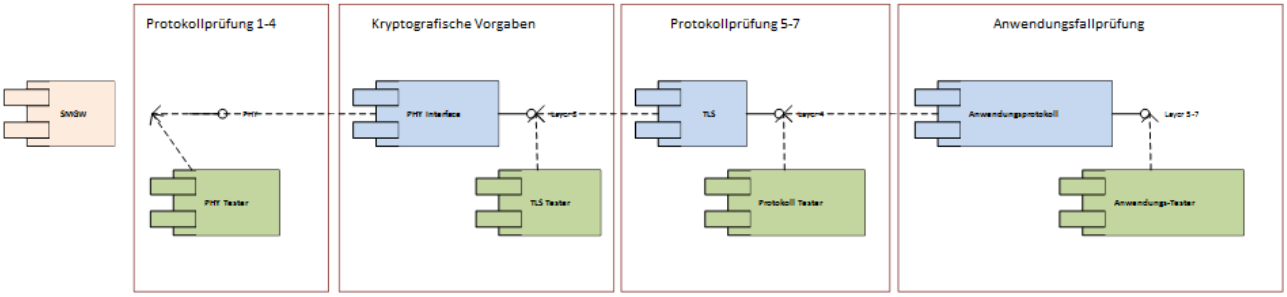

Abbildung 11: Abhängigkeiten zwischen Testmodulen und Unterstützungsmodulen (Bottom-Up-Testverlauf)

In Abbildung 11 wird gezeigt, wie theoretisch schrittweise die Menge von Modulen, die an einem Test beteiligt sind, zu erhöhen wäre, während der Test die OSI-Schichten nach oben abarbeitet. Die Protokoll-bezogenen Tests werden von dem Testmodul „PHY Tester“ durchgeführt. Wenn diese Tests erfolgreich abgeschlossen sind, kann davon ausgegangen werden, dass das SMGW die OSI-Schichten 1-4 so implementiert, wie von der TR gefordert wird. Anschließend wird das Testmodul für den Bereich „OSI-Schichten 1-4“ durch ein Unterstützungsmodul ersetzt, dass die Nutzung dieser Schichten transparent dem nächsten Testmodul („TLS Tester“) zur Verfügung stellt. Diese Vorgehensweise wäre solange fortzusetzen, bis alle Tests abgeschlossen oder definierte Testabbruchkriterien eingetreten sind.

Da es insbesondere für untere Protokollschichten regelmäßig nicht praktikabel sein wird, entsprechende Testdaten für die Protokollschicht zu formulieren, wird auf die Formulierung valider Testdaten auf höherer, vorzugsweise oberster OSI-Schicht zurückgegriffen. Über geeignete PCO-Setzung können dann die erwarteten Testergebnisse auch für die unteren Protokollschichten überprüft werden. Gleichzeitig wird so die Anzahl der insgesamt erforderlichen Testfälle begrenzt, ohne die Testabdeckung zu beeinträchtigen.[21]

Die Reihenfolge der Tests sollte so gewählt werden, dass eindeutig erkennbar ist, auf welcher Schicht ein Fehlverhalten aufgetreten ist.

Die Test- und Unterstützungsmodule müssen nicht notwendigerweise separate Komponenten sein. Es können auch Produkte verwendet werden, die das Verhalten und die Schnittstellen mehrerer Module in sich vereinen.

21 Vgl. dazu auch Hinweise zum Top-Down-Testansatz in Kapitel 5

3 Protokolle

Kapitel 3 beschreibt die an den Schnittstellen WAN, HAN und LMN durchzuführenden Konformitätstests zum Nachweis der anforderungsgemäßen Umsetzung der in [BSI TR-03109-1] vorgegebenen Protokolle. Für jede Schnittstelle orientiert sich die Gliederung dabei am Schichtenmodell des OSI-Standards.[22]

3.1 Schnittstellenübergreifend

Dieses Kapitel beschreibt protokollbezogene Testelemente, die an mehreren oder allen spezifizierten Schnittstellen in gleicher (Grund-) Ausprägung implementiert sein müssen.

Schnittstellenspezifische Anforderungen (Zusätze, Einschränkungen) werden in den jeweiligen Schnittstellen-Kapiteln betrachtet.

3.1.1 Dokumentationsprüfungen (statische Testfälle)

Dieses Kapitel gibt Hinweise auf die übergreifend zu formulierenden statischen Testfälle, die vor den Black-Box-Tests auszuführen sind.

Neben der Überprüfung der Testeingangskriterien laut Kapitel 2.3 sind zu folgenden Punkten detaillierte Dokumentationsprüfungen als statische Testfälle durchzuführen:

- Das Testobjekt verfügt über eine hinreichende Dokumentation (Installations- und Einbauanweisung, Bedienungsanweisung u. ä.) zur Durchführung der Konformitätstests. Der benötigte Dokumentationsumfang leitet sich dabei testobjektspezifisch her aus:
    - den in der TS beschriebenen (anderen) statischen und dynamischen Testfällen,
    - der vom Hersteller gewählten Konstruktion / Bauart des SMGW (bspw. in Bezug auf die Art und Weise der Benutzerschnittstelle) und
    - der Implementierung bzw. Nicht-Implementierung als optional eingestufter Anforderungen der [BSI TR-03109-1].

3.1.2 TLS

Dieses Kapitel beschreibt das Vorgehen für den Test der TLS-Implementierung an den Schnittstellen WAN, HAN und LMN im Hinblick auf die schnittstellenübergreifend zu erfüllenden Anforderungen.

3.1.2.1 Schnittstellenspezifische Kennwerte

In [BSI TR-03116-3] werden die schnittstellenspezifischen Anforderungen an TLS in jeweils separaten Kapiteln beschrieben. In diesem Testkonzept wurde stattdessen eine tabellarische Gegenüberstellung der unterschiedlichen Anforderungen gewählt, um einen besseren Überblick zu gewährleisten. Auf Erläuterungen wie in [BSI TR-03116-3] wird verzichtet.

Es werden bei allen Schnittstellen die gleichen Testfälle ausgeführt, jeweils mit Anpassungen an die schnittstellenspezifischen Anforderungen. So werden bspw. im WAN keine Tests ausgeführt, bei denen das SMGW als TLS Server agieren muss. Insofern werden die schnittstellenspezifischen Anforderungen als Parameter für den schnittstellenübergreifenden Testbereich „TLS“ behandelt.

22 Hinweis: Die abgestimmte Gliederung der Kapitel 3 und 4 ist ähnlich auch in [TSE-MT], Kapitel 4, skizziert.

Anforderung	WAN	HAN	LMN
Maximale Lebensdauer einer Sitzung	48 Stunden	-	1 Monat
Maximale Datenmenge pro Sitzung	-	-	5 MB (5.000.000 Byte, vgl. DIN EN 80000-13:2009-01)
Authentifizierung	gegenseitig, zertifikatsbasiert	gegenseitig zertifikatsbasiert oder serverseitig zertifikatsbasiert und clientseitig HTTP Digest (RFC 2617)	gegenseitig, zertifikatsbasiert
Rolle des SMGW	Client	Client oder Server	Client oder Server
Lebensdauer Zertifikate	vgl. TR-03109-4, Abschnitt 3.2	Zählerzertifikat 5 Jahre, SMGW-Zertifikat 5 Jahre	Zählerzertifikat 7 Jahre, SMGW-Zertifikat 7 Jahre

Tabelle 18: Schnittstellenspezifische Parameter TLS

3.1.2.2 Anforderungen der TR

Die nachfolgend aufgeführten Anforderungen werden in der TR explizit an die TLS-Implementierung eines SMGW gestellt.

ID	Anforderung (abstrakt)	Konkretisierung [BSI TR-03109-1], [BSI TR-03109-3]/[BSI TR-03116-3]	Zusätzliche Referenz(en)
	Übergreifende Anforderung	*Anforderung*	*Anforderungsquelle*
ALL.SEC.01	Kommunikations-verbindungen müssen mit TLS abgesichert werden.	-	[BSI TR-03109-1]
ALL.SEC.01.01	ALL.SEC.01	Mindestens TLS 1.2 muss verwendet werden.=> Das Feld `TLSPlaintext.version` muss den Wert `{3,3}` oder höher haben	[BSI TR-03109-3]
ALL.SEC.01.02	ALL.SEC.01	Ein Rückfall auf niedrigere TLS-Versionen ist nicht zulässig. => Wenn `TLSPlaintext.version` einen kleineren Wert als `{3,3}` hat, muss die Verbindung mit `protocol_version` beendet werden.	[BSI TR-03109-3]
ALL.SEC.01.03	ALL.SEC.01	Eine TLS-Session darf (inklusive eventueller Session Resumptions) maximal 48 Stunden aktiv sein. => Der Versuch, eine Session ID nach 48h zu verwenden, muss zu einen vollständigen Handshake mit einer neuen Session ID führen.	[BSI TR-03116-3]

ID	Anforderung (abstrakt)	Konkretisierung [BSI TR-03109-1], [BSI TR-03109-3]/[BSI TR-03116-3]	Zusätzliche Referenz(en)
	Übergreifende Anforderung	*Anforderung*	*Anforderungsquelle*
ALL.SEC.01.04	ALL.SEC.01	Es MÜSSEN zu einem Zeitpunkt zwei oder mehr TLS-Verbindungen zwischen SMGW und SMGW Administrator gleichzeitig existieren können	[BSI TR-03109-1]
ALL.SEC.01.05	ALL.SEC.01	Es darf kein Session Renegotiation möglich sein => Das Senden eines `ClientHello` nach erfolgreichem Handshake oder eines `HelloRequest` muss ignoriert oder mit einem `no_renegotiation` beantwortet werden.	[BSI TR-03116-3]
ALL.SEC.01.06	ALL.SEC.01	Innerhalb der erlaubten Session-Lebensdauer ist Session-Resumption erlaubt	[BSI TR-03116-3]
ALL.SEC.01.07	ALL.SEC.01	Im Falle einer Stateless Resumption sind dabei die Anforderungen aus [RFC5077], zu beachten	[BSI TR-03116-3] => [RFC5077]
ALL.SEC.01.08	ALL.SEC.01	Als Encoding für die Punkte der elliptischen Kurven soll das Uncompressed Encoding gemäß [BSI TR-03111] verwendet werden. => Seitens des SMGW muss immer `ECPointFormatList==ECPointFormat.uncompressed` sein.	[BSI TR-03116-3] => [BSI TR-03111], [RFC4492]
ALL.SEC.01.09	ALL.SEC.01	Compression ist nicht erlaubt => Seitens des SMGW muss immer `ClientHello.compression_methods==CompressionMethod.null` bzw. `ServerHello.compression_method==CompressionMethod.null` sein.	BSI[23]
ALL.SEC.01.10	ALL.SEC.01	Es sind nur bestimmte NIST-/Brainpool-Kurven erlaubt. Ein Rückfall (fall back) ist nicht zulässig => `EllipticCurveList.NamedCurve` darf nur folgende Werte enthalten: `NamedCurve.secp256r1`, `NamedCurve.secp384r1`, `NamedCurve.brainpoolP256r1`, `NamedCurve.brainpoolP384r1`, `NamedCurve.brainpoolP512r1`	[BSI TR-03116-3], [RFC5639], [RFC4492], [RFC7027]

23 Anforderung wurde seitens BSI im Rahmen der Abstimmung zur vorliegenden Konzeption aufgestellt, findet sich jedoch (aktuell) nicht in der TR.

ID	Anforderung (abstrakt)	Konkretisierung [BSI TR-03109-1], [BSI TR-03109-3]/[BSI TR-03116-3]	Zusätzliche Referenz(en)
	Übergreifende Anforderung	*Anforderung*	*Anforderungsquelle*
ALL.SEC.01.11	ALL.SEC.01	Ausschließlich folgende Cipher Suites dürfen unterstützt werden: `TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256`, `TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384`, `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`, `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384` `=>ServerHello.CipherSuite` darf keinen anderen Eintrag haben. Wenn eine andere Cipher Suite angeboten wird, muss die Verbindung mit `insufficient_security` beendet werden	[BSI TR-03116-3]
ALL.SEC.01.12	ALL.SEC.01	Mindestens folgende Cipher Suite muss unterstützt werden: `TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 =>` `ServerHello.CipherSuite` muss mindestens diesen Eintrag haben.	[BSI TR-03116-3]
ALL.SEC.01.13	ALL.SEC.01	Positivtest: Das SMGW muss gültige Zertifikate, die der TR entsprechen, akzeptieren	[BSI TR-03109-1]
ALL.SEC.01.14	ALL.SEC.01	Negativtest: Das SMGW darf ungültige Zertifikate oder Zertifikate, die nicht der TR entsprechen, nicht akzeptieren. Es muss die entsprechend korrekte Fehlermeldung erzeugt werden (`bad_certificate`, `unsupported_certificate`, `certificate_revoked`, `certificate_expired`, `certificate_unknown`, `unknown_ca`, `access_denied`)	[BSI TR-03109-1] [BSI TR-03116-3]

Tabelle 19: Anforderungen TLS

3.1.2.3 Anforderungen gemäß [RFC5246]

Dieses Kapitel (3.1.2.3) hat informativen Charakter.

Grundsätzlich werden explizit in der Bezugsdokumentation aufgeführte Anforderungen als Quelle für Konformitätstestfälle herangezogen. Aus fachlicher Sicht und unter den Annahmen

- Es wird keine etablierte TLS-Implementierung verwendet, sondern TLS wird neu implementiert.
- Ein implizierter Test von TLS über andere Funktionalitäten ist nicht ausreichend, um eine Aussage über die Interoperabilität zu machen.

509 kann es sinnvoll sein, auch für die Anforderung aus [RFC5246] Testfälle zu entwickeln.

510 Es ist auch praktisch nicht möglich, einen sinnvollen Teilbereich aus [RFC5246] zu extrahieren, ohne dabei
511 willkürlich auf Anforderungen der RFC zu verzichten. Aus diesem Grund werden die [RFC5246]-
512 Anforderungen in diesem Abschnitt als möglicher Testbereich mit aufgenommen. Es ist zu klären, ob
513 tatsächlich Testfälle zu [RFC5246] in die Konformitätsprüfung nach [BSI TR-03109] aufzunehmen sind.

Für [BSI TR-03109-TS-1] ist bisher nicht vorgesehen, diese Testbereiche weiter auszuformulieren.

ID	Anforderung (abstrakt)	Konkretisierung [RFC5246]	Zusätzliche Referenz(en)
	Übergreifende Anforderung	*Anforderung*	*Anforderungsquelle*
RFC5246.01	TLS Record Protocol	-	[RFC5246]
RFC5246.01.01	TLS Record Protocol	Fragmentation	[RFC5246]
RFC5246.01.02	TLS Record Protocol	Record Payload Protection	[RFC5246]
~~RFC5246.01.03~~	TLS Record Protocol	~~Record Compression and Decompression~~	~~[RFC5246]~~[24]
RFC5246.02	TLS Change Cipher Specification Protocol	-	[RFC5246]
RFC5246.03	TLS Alert Protocol	-	[RFC5246]
RFC5246.03.01	TLS Alert Protocol	Closure Alerts	[RFC5246]
RFC5246.03.02	TLS Alert Protocol	Error Alerts	[RFC5246]
RFC5246.04	TLS Handshake Protocol	-	[RFC5246]
RFC5246.04.01	TLS Handshake Protocol	Aufbau und Inhalt der Hello-Pakete; Reaktion des SMGW auf nicht zulässige Inhalte; Reaktion auf Renegotiation wird hier nicht getestet. Folgende Extensions müssen unterstützt werden: `max_fragment_length(0)` `elliptic_curves(10)`, `ec_point_formats(11)`, `signature_algorithms(13)`	[RFC5246], [RFC4366], [RFC4492]
RFC5246.04.02	TLS Handshake Protocol	ServerCertificate (Test der Eigenschaften der Nachricht als auch des Zertifikats)	[RFC5246]
RFC5246.04.03	TLS Handshake Protocol	ServerKeyExchange (entspricht der vom SMGW übertragene Key der ausgewählten CipherSuite, verändert sich der Key?)	[RFC5246]
RFC5246.04.04	TLS Handshake Protocol	CertificateRequest (Werden die richtigen Daten vom Client abgefragt bzw. liefert das SMGW die richtigen Daten? Wie verhält sich das SMGW, wenn nicht die richtigen Daten abgefragt werden?)	[RFC5246], [RFC4492]
RFC5246.04.05	TLS Handshake Protocol	ClientCertificate (vgl. RFC5246.04.02)	[RFC5246]
RFC5246.04.06	TLS Handshake Protocol	ClientKeyExchange (vgl. RFC5246.04.03)	[RFC5246]

24 Diese Anforderung wäre nicht abzuprüfen, da durch ALL.SEC.01.09 verboten.

ID	Anforderung (abstrakt)	Konkretisierung [RFC5246]	Zusätzliche Referenz(en)
	Übergreifende Anforderung	*Anforderung*	*Anforderungsquelle*
RFC5246.04.07	TLS Handshake Protocol	CertificateVerify (Test ob der Wert von `handshake_messages` korrekt ist und ob das SMGW bei falschem Wert die Verbindung beendet)	[RFC5246]
RFC5246.04.08	TLS Handshake Protocol	Finished (Test ob die Berechnung von `verify_data` und der Wert von `finished_label` korrekt sind und ob das SMGW bei falscher Berechnung die Verbindung beendet)	-

Tabelle 20: Anforderungen TLS aus [RFC5246]

514 3.1.2.4 Nicht von [BSI TR-03109-TS-1] betrachtete Anforderungen

In diesem Unterkapitel können die Ergebnisse der Entscheidung zum Testumfang für eine TLS-Implementierung (vgl. Einführung zu Kapitel 3.1.2.3) sowie als „nicht mit den definierten Testmethoden testbare Anforderungen“ aus [BSI TR-03109-1] aufgenommen werden (Ergebnis der Arbeitspakete 2 und 3). Aktuell werden diese Informationen – soweit bereits bekannt – in Anlage C geführt.

ID	Anforderung (Kurzbeschreibung)	Erläuterung der Einschränkung
zu definieren	zu definieren	-

Tabelle 21: Anforderungen außerhalb des Testumfangs von [BSI TR-03109-TS-1]

515 Durch die Tests nach [BSI TR-03109-TS-1] nicht prüfbare Anforderungen können möglicherweise im
516 Rahmen der CC-Evaluierung untersucht werden. Ggf. muss dies individuell für jeden Prüfauftrag betrachtet
517 werden.

518 3.1.2.5 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitätsvor-gaben	Gewichtung (A ... C laut Tabelle 8)	A	Die geforderte Funktionalität impliziert entsprechende Interoperabilität auf der betrachteten OSI-Schicht.
1	Funktionalitätsvorga-ben	Gewichtung (A ... C laut Tabelle 8)	A	-
2	TR-spezifische Anfor-derung	Auswahl (ja oder nein)	nein	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurationsmög-lichkeiten	Gewichtung (A ... C laut Tabelle 8)	A	-
2	Informativ: bekannte Sicherheitsri-siken und Angriffsszе-narien	Auswahl (ja oder nein)	ja	-
2	Testbarkeit mit be-kannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	A	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 22: Bewertungskriterien für TLS

519 3.1.2.6 Testeingangskriterien, Abhängigkeiten

520 Es müssen nachweislich die Funktionen des SecMod entsprechend [BSI TR-03109-2] zur Verfügung stehen.

521 Eine – ggf. durch die Testinfrastruktur bereitzustellende – Implementierung der OSI-Protokollschichten 1-
522 4 muss vorhanden sein.

523 3.1.2.7 Testdurchführung

524 Es werden die vorgesehenen statischen (3.1.2.7.1) und dynamischen (3.1.2.7.2) Tests beschrieben.

525 Für die dynamischen Tests zur Interoperabilität wird dabei zwischen Anforderungen der TR (insbesondere
526 [BSI TR-03116-3]) und Anforderungen aus referenzierten Standards, die explizit Testfokus sind,
527 unterschieden.

528 3.1.2.7.1 Dokumentationstests

529 Nachfolgende Tabelle gibt eine Übersicht über die vorzusehenden Tests, in denen zu erfüllende
530 Anforderungen anhand von Dokumentationsprüfungen durchgeführt werden.

Die Inhalte des Dokumentationstests sind abhängig von der Festlegung zum Anforderungsumfang für [BSI TR-03109-TS-1].

Anforderungs-referenz	Testfokus, zu prüfendes Dokument	Durchführung anhand von (Referenzpunkt)	Erwarteter Inhalt
Zu definieren	ICS	Zu definieren	• Angaben zur Implementierung wie ICS-Formular beschrieben

Tabelle 23: Testdurchführung – Dokumentationsprüfung TLS

532 Die Dokumentationstests sind vor den dynamischen Tests auszuführen.

533 3.1.2.7.2 Dynamische Tests

534 3.1.2.7.2.1 Dynamische Tests zu 3.1.2.2

535 Nachfolgende Tabelle gibt eine Übersicht über die vorzusehenden Tests zu funktionalen Anforderungen.

Anforderungs-referenz	Testfokus	Durchführung	Erwartetes Verhalten
ALL.SEC.01.03	Dauer einer TLS Session	Halten einer TLS Session	Der Versuch, eine Session ID nach 48h zu verwenden, muss zu einen vollständigen Handshake mit einer neuen Session ID führen.
ALL.SEC.01.05	Session Renegotiation	Versuch, in einer Session eine Renegotiation zu initiieren	Der Versuch muss vom SMGW mit `no_renegotiation` beantwortet werden
ALL.SEC.01.06	Session Resumption	Versuch, eine alte Session fortzusetzen	Die alte Session kann fortgesetzt werden, so lange die Session noch nicht 48h alt ist.
ALL.SEC.01.07	Stateless Resumption	Versuch, eine Sitzung gem. [RFC5077] (ohne Server-gespeicherten Zustand) fortzusetzen	Anforderungen von [RFC5077], insbes. Kap.5, müssen eingehalten werden[25]

Tabelle 24: Testdurchführung – funktionale Aspekte TLS

536 Nachfolgende Tabellen geben eine Übersicht über die vorzusehenden Tests zu den Interoperabilitäts-
537 aspekten.

25 Punkt muss im Verlauf des Projektes noch genauer spezifiziert werden.

Anforderungs-referenz	Testfokus	Durchführung	Erwartetes Verhalten
ALL.SEC.01.01	eingesetzte TLS Version	Durchführung eines TLS Handshake	vom SMGW eingesetzte Protokollversion ist mindestens 1.2
ALL.SEC.01.02	akzeptierte TLS-Version	Durchführung eines TLS-Handshake	niedrigere Protokollversionen als 1.2 werden vom SMGW abgelehnt
ALL.SEC.01.04	Anzahl der gleichzeitigen TLS-Verbindungen	Aufbau einer zweiten TLS-Verbindung	Es ist möglich, eine zweite TLS-Verbindung aufzubauen. Sowohl die erste als auch die zweite Session sind weiterhin nutzbar
ALL.SEC.01.08	Uncompressed Encoding	TLS-Handshake mit SMGW	Seitens des SMGW muss immer `ECPointFormatList==ECPointFormat.uncompressed` sein. Andere Kodierungen müssen vom SMGW abgelehnt werden.
ALL.SEC.01.09	compression	TLS-Handshake mit SMGW	Seitens des SMGW muss immer `ClientHello.compression_methods==CompressionMethod.null` bzw. `ServerHello.compression_method==CompressionMethod.null` sein.
ALL.SEC.01.10	Elliptische Kurven	TLS-Handshake mit SMGW	`EllipticCurveList.NamedCurve` darf nur folgende Werte enthalten: `NamedCurve.secp256r1`, `NamedCurve.secp384r1`, `NamedCurve.brainpoolP256r1`, `NamedCurve.brainpoolP384r1`, `NamedCurve.brainpoolP512r1`
ALL.SEC.01.11	erlaubte Cipher Suites	TLS-Handshake mit SMGW	`ServerHello.CipherSuite` darf keinen anderen Eintrag haben. Wenn eine andere Cipher Suite angeboten wird, muss die Verbindung mit `insufficient_security` beendet werden

Anforderungs-referenz	Testfokus	Durchführung	Erwartetes Verhalten
ALL.SEC.01.12	geforderte Cipher Suites	TLS-Handshake mit SMGW	`ServerHello.CipherSuite` muss mindestens den Eintrag `TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256` haben.Wenn das SMGW als Client agiert, muss mindestens diese Cipher Suite akzeptiert werden.
ALL.SEC.01.13	geforderte Zertifikats-eigenschaften	TLS-Handshake mit SMGW	Das SMGW muss gültige Zertifikate, die der TR entsprechen, akzeptieren
ALL.SEC.01.14	verbotene Zertifikats-eigenschaften	TLS-Handshake mit SMGW	Das SMGW darf ungültige Zertifikate oder Zertifikate, die nicht der TR entsprechen, nicht akzeptieren. Es muss die entsprechend korrekte Fehlermeldung erzeugt werden (`bad_certificate`, `unsupported_certificate`, `certificate_revoked`, `certificate_expired`, `certificate_unknown`, `unknown_ca`, `access_denied`)

Tabelle 25: Testdurchführung – Interoperabilität: Anbindung TLS

538 Anmerkung: Als mindestens zu unterstützen ist TLS 1.2 vorgegeben; da höhere Versionen aktuell lediglich
539 in Entwicklung sind, ist „mindestens“ in diesen Fällen als „ausschließlich“ zu verstehen.

540 3.1.2.7.2.2 Dynamische Tests zu 3.1.2.3

541 Dieses Kapitel (3.1.2.7.2.2)hat informativen Charakter.

Nachfolgende mögliche Tests sind bisher nicht für die Aufnahme in die Testspezifikation geplant.

Anforderungs-referenz	Testfokus	Durchführung	Erwartetes Verhalten
RFC5246.01.01	Fragmentation	Es werden Anwendungsnachrichten sowohl fragmentiert als auch kombiniert übertragen	Das SMGW muss die fragmentierten als auch die kombinierten Anwendungs-nachrichten korrekt bearbeiten.
RFC5246.01.02	Record Payload Protection	Es werden Nachrichten mit gültigem und mit ungültigem MAC übertragen	Nachrichten mit gültigem MAC müssen korrekt bearbeitet werden. Bei Nachrichten mit ungültigem MAC muss die Session mit `bad_record_mac` beendet werden.

RFC5246.02	TLS Change_Cipher_Spec_ Protocol	Senden einer ChangeCipherSpec-Nachricht	Wenn vorher ein Pending State ausgehandelt wurde, wird dieser zum Current State. Was passiert, wenn der Pending State leer ist, ist nicht explizit formuliert und wird nicht getestet.
RFC5246.03	TLS Alert Protocol: Empfang	Ob das SMGW Alert Nachrichten so schickt, wie das die RFC fordert, wird über die anderen Anforderungen mit getestet (vgl. jeweiliges Erwartetes Verhalten)	
RFC5246.03	TLS Alert Protocol: Empfang	Senden einer Alert Nachricht	Das SMGW muss so auf die Nachricht reagieren, wie in Abschnitt 7.2 der RFC beschrieben ist. Es wird nicht getestet, wie das SMGW auf `warning`-Nachrichten reagiert, weil die RFC dies offen lässt.
RFC5246.03	TLS Alert Protocol: `close_notify`	Senden von `close_notify`	Sämtliche Nachrichten, die das SMGW nach `close_notify` erhält, müssen ignoriert werden
RFC5246.04.01	TLS Handshake Protocol: ServerHello Extensions	Senden von ClientHello mit verschiedenen Extensions, mindestens jedoch die geforderten	ServerHello.Extension enthält mindestens `max_fragment_length(0), elliptic_curves(10), ec_point_formats(11), signatur_formats(13)`
RFC5246.04.01	TLS Handshake Protocol: ServerHello Extensions	Senden von ClientHello mit verschiedenen Extension, aber nicht mit allen erforderlichen Extensions	Das SMGW antwortet mit `handshake_failure`
RFC5246.04.01	TLS Handshake Protocol: ClientHello Extensions	Wakeup	Das ClientHello des SMGW enthält mindestens `max_fragment_length(0), elliptic_curves(10), ec_point_formats(11), signatur_formats(13)`
RFC5246.04.01	TLS Handshake Protocol	Senden eines gültigen ClientHello	SMGW antwortet mit gültigem ServerHello
RFC5246.04.01	TLS Handshake Protocol	Wakeup	SMGW schickt ein gültiges ClientHello
RFC5246.04.01	TLS Handshake Protocol	Empfang eines gültigen ClientHello vom SMGW, Senden eines gültigen ServerHello	keine Antwortnachricht
RFC5246.04.01	TLS Handshake Protocol	Empfang eines gültigen ClientHello vom SMGW, Senden eines ungültigen ServerHello	Das SMGW antwortet mit `handshake_failure`

RFC5246.04.02	Serverzertifikat	Empfang einer Certificate Nachricht	Es wurde das richtige Zertifikat verwendet, die Eigenschaften des Zertifikats entsprechen von der TR geforderten
RFC5246.04.02	Serverzertifikat	Senden einer gültigen Certificate-Nachricht	keine Antwortnachricht
RFC5246.04.02	Serverzertifikat	Senden einer ungültigen Certificate-Nachricht	Das SMGW antwortet mit `bad_certificate`, `unsupported_certificate`, `certificate_revoked`, `certificate_expired` oder `certificate_unknown`
RFC5246.04.03	ServerKeyExchange	Empfang einer ServerKeyExchange Nachricht	Die Schlüsselparameter entsprechen der ausgewählten Cipher Suite. Das compressed encoding wird nicht verwendet. Der Schlüssel unterscheidet sich von den vorher empfangenen Schlüsseln
RFC5246.04.03	ServerKeyExchange	Senden einer gültigen ServerKeyExchange Nachricht	keine Antwortnachricht
RFC5246.04.03	ServerKeyExchange	Senden einer ungültigen ServerKeyExchange Nachricht (z. B. unpassend zum gewählten `signature_algorithms`-Wert)	Das SMGW antwortet mit `handshake_failure`
RFC5246.04.04	CertificateRequest	Überspringen der `CertificateRequest` Nachricht	<undefiniert>[26]
RFC5246.04.04	CertificateRequest	Senden einer ungültigen `CertificateRequest`-Nachricht	Das SMGW antwortet mit `handshake_failure`
RFC5246.04.04	CertificateRequest	Senden einer gültigen `CertificateRequest` Nachricht	Das SMGW antwortet mit `ClientCertificate`
RFC5246.04.05	ClientCertificate	vgl. ServerCertificate	
RFC5246.04.05	ClientCertificate	Überspringen der ClientCertificate Nachricht	Das SMGW antwortet mit `handshake_failure`
RFC5246.04.06	ClientKeyExchange	vgl. ServerKeyExchange	
RFC5246.04.07	CertificateVerify	Senden einer korrekten CertificateVerify Nachricht	keine Antwort vom SMGW
RFC5246.04.07	CertificateVerify	Überspringen der CertificateVerify Nachricht	<undefiniert>[27]

26 <undefiniert> ... Eine Vorgabe seitens RFC existiert für das Verhalten nicht. Für den SMGW-Kontext wäre jedoch eine Vorgabe u. U. von Bedeutung und müsste durch den TR-Herausgeber dann getroffen werden.

RFC5246.04.07	CertificateVerify	Senden einer unkorrekten CertificateVerify Nachricht	<undefiniert>[28]
RFC5246.04.08	Finished	Überspringen der Finished Nachricht	<undefiniert>[29]
RFC5246.04.08	Finished	Senden einer korrekten Finished Nachricht	die nächste Nachricht hat den type `ContentType.application_data` und benutzt den neu ausgehandelten State
RFC5246.04.08	Finished	Senden einer unkorrekten Finished Nachricht	<undefiniert>[30]
RFC5246.04.08	Finished	Senden einer Finished Nachricht ohne vorherige ChangeCipherSpec Nachricht	Verbindungsabbruch mit einem fatal error

Tabelle 26: Testdurchführung – Interoperabilität: Verbindung TLS

Anforderungs-referenz	Testfokus	Durchführung	Erwartetes Verhalten
RFC5246.01	TLS Nachrichtensyntax: SMGW als Sender	wird implizit getestet, da bei Abweichungen von der spezifizierten Syntax falsche Datenwerte auftreten bzw. der MAC falsch ist	SMGW versendet gültige Nachrichten
RFC5246.01	TLS Nachrichtensyntax: SMGW als Empfänger	Es werden Nachrichten versendet, die sich nicht an die in [RFC5246] spezifizierte Syntax halten	Das SMGW muss die Verbindung mit der entsprechenden Fehlermeldung (`illegal_parameter`, `decode_error`, etc.) beenden
RFC5246.01	TLS Nachrichtengröße: SMGW als Sender	Es wird versucht (über das Anwendungsprotokoll), Nachrichten zu verschicken, die größer sind als `max_fragment_size`	Nachrichten, die größer sind als `max_fragment_size`, müssen fragmentiert werden
RFC5246.01	TLS Nachrichtengröße: SMGW als Empfänger	Versenden von Nachrichten verschiedener Größe	gdw. die Nachrichten größer als max_fragment_size sind, muss das SMGW die Verbindung mit `record_overflow` beenden.

Tabelle 27: Testdurchführung – Syntaktische Interoperabilität TLS

542 3.1.2.8 Testdaten

543 Folgende Testdaten werden benötigt:

27 vgl. 26
28 vgl. 26
29 vgl. 26
30 vgl. 26

Testdaten-forderung	Umzusetzender Standard	Anforderung TR	Hinweise
Anwendungs-daten	entsprechende Standards des darüber liegenden Protokolls	-	Es ist zu testen, dass die maximal zulässige Datenmenge pro Schlüssel nicht überschritten wird.
Cipher Suites	BSI-TR-03116-3	konkrete Cipher Suites	Es sind auch nicht erlaubte Cipher Suites zu testen
Elliptische Kurven	BSI-TR-03116-3	konkrete NIST- und Brainpool-Kurven	Es sind auch andere Kurven zu testen.
Zertifikate	BSI-TR-03116-3	-	-
ECDHE-Schlüssel	BSI-TR-03116-3	-	Es ist zusätzlich zu testen, ob die ECDE-Keys wirklich ephemeral sind

Tabelle 28: Testdatenanforderungen TLS

3.1.2.9 Testinfrastrukturanforderungen, Hinweise zu möglichen Testwerkzeugen (informativ)

Abbildung 12 skizziert beispielhaft für den Aufbau einer TLS-Sitzung, welche Aktionen und Messungen die Testumgebung ausführen muss.

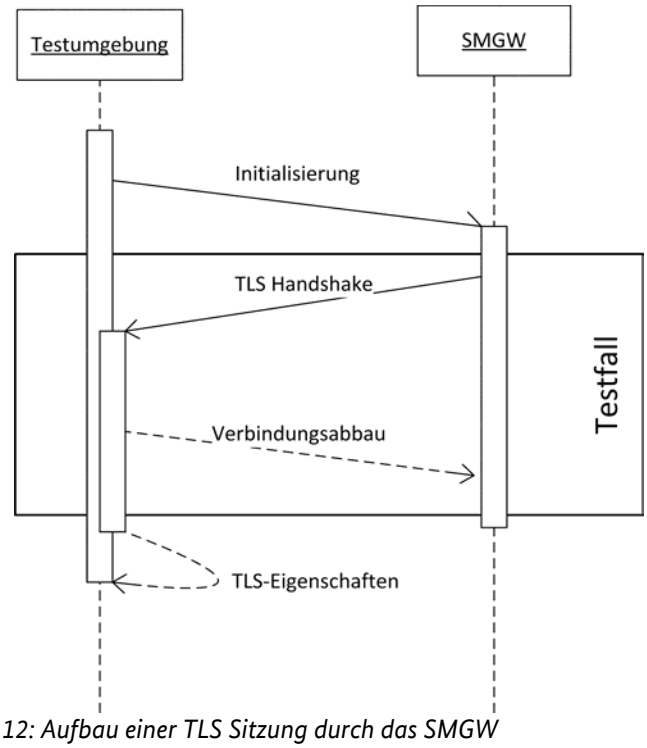

Abbildung 12: Aufbau einer TLS Sitzung durch das SMGW

Nachfolgende Tabelle gibt eine Übersicht über die generisch formulierten Anforderungen an eine Testumgebung.

Umgebungsan-forderung	Umzusetzender Standard	Implementierungsmöglichkeiten
Bereitstellung SecMod	Gemäß Vorgaben aus [BSI TR-03109], insbesondere [BSI TR-03109-2]	Zu beachten: grundsätzlich ist das SecMod im SMGW implementiert. Testvoraussetzung ist neben dem erfolgreichen Bestehen der CC-Evaluierung auch der erfolgreich abgeschlossene Konformitätstest [BSI TR-03109-2]. Für die Tests [BSI TR-03109-TS-1] agiert das SecMod auch als Teil der Testumgebung.
SM-PKI	Gemäß Vorgaben aus [BSI TR-03109]	Eine geeignete PKI muss vorhanden sein.
Bereitstellung TLS-Server / TLS-Client über Simulatoren	Gespiegelt zu den SMGW-Anforderungen	Abhängig vom Anspruch an den Umfang der Tests – es ist denkbar, existierende Produkte einzusetzen (Wireshark, OpenSSL, SSLdump, SSLsnif) oder eine Referenzimplementierung selbst zu erstellen und zu qualifizieren.

Tabelle 29: Testumgebungsanforderungen TLS

551 3.2 WAN

552 Dieses Kapitel erläutert die protokollbezogenen Testelemente an der WAN-Schnittstelle.

553 Zu den zu verwendenden Protokollen der OSI-Schichten 1 bis 4 werden von der [BSI TR-03109-1] keine
554 Vorgaben gemacht. Geeignete Implementierungen der einzelnen Schichten sind durch die Hersteller zu
555 realisieren. Für diese Schichten ergeben sich nach [BSI TR-03109-1] also keine konkreten Testfälle für die
556 WAN-Schnittstelle in der Testspezifikation.

557 Das Testobjekt **muss** die Protokollschichten 1 – 4 derart zur Verfügung stellen, dass ein Konformitätstest für
558 die darüber liegenden Schichten möglich ist (Testeingangskriterium, vgl. 2.3).

559 Folgende Protokolle werden für **die** WAN-Schnittstelle von der [BSI TR-03109-1] vorgegeben und müssen
560 entsprechend geprüft werden:

561 • TLS
562 • HTTP
563 • RESTful COSEM Webservices
564 • CMS Inhaltsdatensicherung
565 • XML Transfersyntax für COSEM Objekte
566 • DLMS/COSEM-IC IEC 62056-6-2
567 • OBIS IEC 62056-6-1

568 3.2.1 TLS

569 Hinweis: die schnittstellenübergreifenden Testaspekte sind 3.1.2 beschrieben.

570 3.2.1.1 Schnittstellenspezifische Besonderheiten

571 Im WAN wird das SMGW nur als TLS-Client eingesetzt. Das bedeutet, dass alle Testfälle, bei denen das
572 SMGW als Server agiert, hier nicht ausgeführt werden. Es wird jedoch getestet, ob das SMGW auf ein
573 ClientHello antwortet.

574 Es wird ausschließlich gegenseitige zertifikatsbasierte Authentifizierung eingesetzt.

575 3.2.1.2 Anforderungen der TR

576 Folgende Anforderungen sind WAN-spezifisch zu beachten:

ID	Anforderung (abstrakt)	Konkretisierung [BSI TR-03109-1], [BSI TR-03109-3]/[BSI TR-03116-3]	Zusätzliche Referenz(en)
	Übergreifende Anforderung	*Anforderung*	*Anforderungsquelle*
ALL.SEC.01.03	ALL.SEC.01	Eine TLS-Session darf (inklusive eventueller Session Resumptions) maximal 48 Stunden aktiv sein. => Der Versuch, eine Session ID nach 48h zu verwenden, muss zu einen vollständigen Handshake mit einer neuen Session ID führen.	[BSI TR-03116-3]

ID	Anforderung (abstrakt)	Konkretisierung [BSI TR-03109-1], [BSI TR-03109-3]/[BSI TR-03116-3]	Zusätzliche Referenz(en)
	Übergreifende Anforderung	*Anforderung*	*Anforderungsquelle*
ALL.SEC.01.04	ALL.SEC.01	Es MÜSSEN zu einem Zeitpunkt zwei oder mehr TLS-Verbindungen zwischen SMGW und SMGW Administrator gleichzeitig existieren können	[BSI TR-03109-1]
ALL.SEC.01.05	ALL.SEC.01	Es darf kein Session Renegotiation möglich sein => Das Senden eines `ClientHello` nach erfolgreichem Handshake oder eines `HelloRequest` muss ignoriert oder mit einem `no_renegotiation` beantwortet werden.	[BSI TR-03116-3]
ALL.SEC.01.06	ALL.SEC.01	Innerhalb der erlaubten Session-Lebensdauer ist Session-Resumption erlaubt	[BSI TR-03116-3]
ALL.SEC.01.07	ALL.SEC.01	Im Falle einer Stateless Resumption sind dabei die Anforderungen aus [RFC5077], insbesondere Kapitel 5, zu beachten	[BSI TR-03116-3] => [RFC5077]
ALL.SEC.01.08	ALL.SEC.01	Als Encoding für die Punkte der elliptischen Kurven soll das Uncompressed Encoding gemäß [BSI TR-03111] verwendet werden. => Seitens des SMGW muss immer `ECPointFormatList==ECPointFormat.uncompressed` sein.	[BSI TR-03116-3] => [BSI TR-03111], [RFC4492]
ALL.SEC.01.09	ALL.SEC.01	Compression ist nicht erlaubt => Seitens des SMGW muss immer `ClientHello.compression_methods==CompressionMethod.null` bzw. `ServerHello.compression_method==CompressionMethod.null` sein.	BSI
ALL.SEC.01.10	ALL.SEC.01	Es sind nur bestimmte NIST-/Brainpool-Kurven erlaubt. Ein Rückfall (fall back) ist nicht zulässig => `EllipticCurveList.NamedCurve` darf nur folgende Werte enthalten: `NamedCurve.secp256r1`, `NamedCurve.secp384r1`, `NamedCurve.brainpoolP256r1`, `NamedCurve.brainpoolP384r1`, `NamedCurve.brainpoolP512r1`	[BSI TR-03116-3], [RFC5639], [RFC4492], [RFC7027]

ID	Anforderung (abstrakt)	Konkretisierung [BSI TR-03109-1], [BSI TR-03109-3]/[BSI TR-03116-3]	Zusätzliche Referenz(en)
	Übergreifende Anforderung	*Anforderung*	*Anforderungsquelle*
ALL.SEC.01.11	ALL.SEC.01	Ausschließlich folgende Cipher Suites dürfen unterstützt werden: `TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256`, `TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384`, `TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256`, `TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384` `=>ServerHello.CipherSuite` darf keinen anderen Eintrag haben. Wenn eine andere Cipher Suite angeboten wird, muss die Verbindung mit `insufficient_security` beendet werden	[BSI TR-03116-3]
ALL.SEC.01.12	ALL.SEC.01	Mindestens folgende Cipher Suite muss unterstützt werden: `TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 =>` `ServerHello.CipherSuite` muss mindestens diesen Eintrag haben.	[BSI TR-03116-3]
ALL.SEC.01.13	ALL.SEC.01	Positivtest: Das SMGW muss gültige Zertifikate, die der TR entsprechen, akzeptieren	[BSI TR-03109-1]
ALL.SEC.01.14	ALL.SEC.01	Negativtest: Das SMGW darf ungültige Zertifikate oder Zertifikate, die nicht der TR entsprechen, nicht akzeptieren. Es muss die entsprechend korrekte Fehlermeldung erzeugt werden (`bad_certificate`, `unsupported_certificate`, `certificate_revoked`, `certificate_expired`, `certificate_unknown`, `unknown_ca`, `access_denied`)	[BSI TR-03109-1] [BSI TR-03116-3]

Tabelle 30: Anforderungen WAN / TLS

577 3.2.1.3 Testdurchführung

578 3.2.1.3.1 Dynamische Tests

579 Folgende schnittstellenspezifischen dynamischen Tests sind neben den schnittstellenübergreifend
580 vorgegebenen Tests erforderlich:

Anforderungs-referenz	Testfokus	Durchführung	Erwartetes Verhalten
RFC5246.04.04	CertificateRequest	Empfang einer CertificateRequest Nachricht	`certificate_types` und `supported_signature_algorithms` müssen den Anforderungen der TR entsprechen. `certificate_authorities` muss ausschließlich den DN der Sub-CA enthalten
RFC5246.04.05	ClientCertificate	Senden einer leeren ClientCertificate Nachricht	Abbruch der Verbindung mit `handshake_failure`

Tabelle 31: Testdurchführung WAN / TLS – Interoperabilität: Verbindung

581 3.2.2 HTTP

582 Die Prüfung der korrekten Implementierung des HTTP-Protokolls [RFC2616] umfasst Testfälle für die
583 HTTP Verben, die HTTP Header-Felder, den HTTP Body, die HTTP-Status-Codes und der HTTP Version.

584 3.2.2.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitätsvorgaben	Gewichtung (A ... C laut Tabelle 8)	A	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	C	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	ja	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	A	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	A	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 32: Bewertungskriterien für WAN / HTTP

3.2.2.2 HTTP Verben

Die Webservice-Anbieter SMGW, SMGW Administrator und EMT **müssen** die folgenden Dienste nach [BSI TR-03109-1/AII] anbieten:

Kommunikations-szenario	Webservice-Benutzer	Webservice-Anbieter	Dienste

MANAGEMENT	SMGW Administrator	*SMGW*	`Get`
			`Set`
			`Action`
			`Create`
			`Delete`
			`Notify`

ADMIN-SERVICE	*SMGW*	SMGW Administrator	`Get`
			`Set`
			`Action`
			`Notify`

INFO-REPORT	*SMGW*	EMT	`Get`
			`Set`
			`Action`
			`Notify`

Tabelle 33: Durch Webservice-Anbieter anzubietende Dienste, Testobjekt in *kursiv*

Die korrekte Implementierung der HTTP-Verben kann nur geprüft werden, wenn das Testobjekt SMGW als Webservice-Anbieter agiert. Aus diesem Grund wird nachfolgend nur das Kommunikationsszenario MANAGEMENT betrachtet und getestet.

In der nachfolgenden Tabelle sind die anzubietenden Dienste, die zu verwendenden HTTP-Verben und die Request-/Response-Parameter zusammengefasst dargestellt:

Dienst	HTTP-Verb	Request-URI enthält	Request-Body enthält	Response-Body enthält
`Get`	`GET`	Container-, Objekt-, Attribut-Deskriptor	Leer	Container-, Objekt- oder Attribut-Werte
`Set`	`PUT`	Container-, Objekt-Attribut-Deskriptor	Container-, Objekt- oder Attribut-Werte	Leer
`Action`	`POST`	Objekt-, Methoden-Deskriptor	Methoden Aufruf-Werte	Methoden Antwort-Werte
`Create`	`PUT`	Container-, Objekt-Deskriptor	Container-, Objekt- oder Attribut-Werte	Leer
`Delete`	`DELETE`	Container-, Objekt-Deskriptor	Leer	Leer
`Notify`	`POST`	Methoden-Deskriptor	Event-Parameter	Leer

Tabelle 34: Dienste, HTTP-Verben und Request-/Response-Parameter

Um zu prüfen, ob ein Dienst beim Webservice-Anbieter korrekt implementiert wurde, wird ein gültiger Request an den Endpunkt des Webservice-Anbieters gesendet. Ein gültiger Request muss folgende Elemente enthalten:

- HTTP Verb für den jeweiligen Dienst („GET“, „PUT“, „POST“, „DELETE“)

- URI (die anzusprechende Ressource)
- HTTP Version („HTTP/1.1“)
- HTTP-Header („Content-Length“, „Host“, weitere Header-Felder sind optional und vom Dienst abhängig)
- HTTP-Body (optional, abhängig vom Dienst)

Beispiel für einen gültigen HTTP-Request:

```
GET https://ebsi0012345678.sm.bsi.bund.de:14059
/smgw/cosem/ldevs/ebsi0a12345678.sm/objects/3-
0100010801ff/attributes/1 HTTP/1.1
Host: ebsi0012345678.sm.bsi.bund.de:14059
Content-Length: 100
```

Der Webservice-Anbieter muss mit einer gültigen Response antworten. Die gültige Response muss folgende Elemente enthalten:

- HTTP-Status-Code („200“)
- HTTP-Header (optional und vom Dienst/Request abhängig)
- HTTP-Body (optional, abhängig vom Dienst)

Beispiel für eine gültige HTTP-Response:

```
HTTP/1.1 200 OK
Content-Type: application/vnd.de-dke-k461-cosem +xml;encap=cms-
tr03109
Content-Encoding: deflate
Content-Length: 2000
<CMS encoded and signed body>
```

3.2.2.3 HTTP Header-Felder

Der Webservice-Anbieter **muss** nach [BSI TR-03109-1/AII] einen Teil der Standard HTTP-Header und weitere TR-spezifische HTTP-Header implementieren. Diese Anforderungen sind in den folgenden beiden Tabellen aufgelistet.

Name	muss / kann / bedingt	RFC/spezifisch und Beschreibung
`Content-Type`	bedingt	[RFC2616] Sofern ein Request-Body nach dieser Spezifikation vorhanden ist, ist dieser Header verpflichtend. Gibt den Typ des Request-Body an.
`Content-Encoding`	bedingt	[RFC2616] Sofern ein Request-Body vorhanden ist, ist dieser Header verpflichtend, falls ein Content-Encoding angewandt wurde (wie z. B. Kompression)
`Content-Length`	muss[31]	[RFC2616] Gibt die Länge des Request-Body in Bytes an.
`Host`	muss	[RFC2616] Identifiziert den Host an den die Anfrage gerichtet ist. Dies entspricht der Host-Identifikation aus der HTTP-URI.
`Accept`	kann	[RFC2616] Teilt dem Webservice-Anbieter mit, welche Content-Types im Body einer Response erlaubt sind.
`Accept-Encoding`	kann	[RFC2616] Teilt dem Webservice-Anbieter mit, welche Content-Encodings im Body einer Response erlaubt sind.
`Range`	kann	[RFC2616] Teilt dem Webservice-Anbieter mit welcher Teil einer Ressource übertragen werden soll.
`x-CID`	kann	TR-spezifisch Correlation-ID zwischen Anfrage und Antwort. Dies ist besonders für asynchrone Antworten notwendig.
`x-ContactURI`	kann	TR-spezifisch URI, an die bei Asynchronen Responses der Notify-Request zugestellt werden kann.

Tabelle 35: HTTP-Header für Request

31 Mit dem Herausgeber der TR in Klärung, ob „muss“ lediglich dann umzusetzen ist, wenn ein message-body vorhanden ist.

Name	muss / kann / bedingt	RFC/spezifisch und Beschreibung
`Content-Type`	bedingt	[RFC2616] Sofern ein Response-Body nach dieser Spezifikation vorhanden ist, ist dieser Header verpflichtend. Gibt den Typ des Response-Body an.
`Content-Encoding`	bedingt	[RFC2616] Sofern ein Response-Body vorhanden ist, ist dieser Header verpflichtend, falls ein Content-Encoding angewandt wurde (wie z. B. Kompression)
`Content-Length`	bedingt	[RFC2616] Gibt die Länge des Response-Body in Bytes an.
`Content-Range`	kann	[RFC2616] Teilt dem Client mit, welcher Teil (Byte-Range) bei einer mit Range fragmentierten Anfrage in der Response geliefert wird.

Tabelle 36: HTTP-Header für Response

Es werden Positiv- und Negativtestfälle spezifiziert.

Bei den Positivtestfällen werden gültige Requests an den Endpunkt des Webservice-Anbieters gesendet. Diese enthalten im HTTP-Header verschiedene gültige Kombinationen von Header-Feldern. Gültige Kombinationen ergeben sich aus den zur Verfügung stehenden Diensten beim Webservice-Anbieter und aus der [BSI TR-03109-1/AII].

Ein gültiger Request muss folgende Elemente enthalten:

- HTTP-Verb für den jeweiligen Dienst („GET“, „PUT“, „POST“, „DELETE“)
- URI (die anzusprechende und vorhandene Ressource)
- HTTP-Version („HTTP/1.1“)
- HTTP-Header („Content-Length“, „Host“, weitere gültige Header-Felder in Abhängigkeit vom Dienst)
- HTTP-Body (optional, abhängig vom Dienst)

Beispiel für einen gültigen HTTP-Request:

```
PUT https://ebsi0012345678.sm.bsi.bund.de:14059
/smgw/cosem/ldevs/ebsi0a12345678.sm/objects/3-
0100010801ff[32]/attributes/1 HTTP/1.1
Host: ebsi0012345678.sm.bsi.bund.de:14059
Content-Type: application/vnd.de-dke-k461-cosem +xml;encap=cms-
tr03109
Content-Encoding: deflate
Content-Length: 1000
```

32 Der Herausgeber der TR prüft derzeit, ob explizit Systemobjekte für den Test verwendet werden sollen.

```
<CMS encoded and signed body>
```

Der Webservice-Anbieter muss mit einer gültigen Response antworten. Die gültige Response muss folgende Elemente enthalten:

- HTTP-Status-Code („200“)
- HTTP-Header (optional und vom Dienst/Request abhängig)
- HTTP-Body (optional, abhängig vom Dienst)

Beispiel für eine gültige HTTP-Response:

```
HTTP/1.1 200 OK
```

Bei den Negativtestfällen werden ungültige Requests an den Endpunkt des Webservice-Anbieters gesendet. Diese enthalten im HTTP-Header verschiedene ungültige Kombinationen von Header-Feldern. Ungültige Kombinationen ergeben sich aus den zur Verfügung stehenden Diensten beim Webservice-Anbieter und aus der [BSI TR-03109-1/AII].

Beispiel für einen ungültigen HTTP-Request:

```
SET https://ebsi0012345678.sm.bsi.bund.de:14059
/smgw/cosem/ldevs/ebsi0a12345678.sm/objects/3-
0100010801ff/attributes/1 HTTP/1.1
Host: ebsi0012345678.sm.bsi.bund.de:14059
Content-Length: 1000
<CMS encoded and signed body>
```

Der Webservice-Anbieter muss mit einer gültigen Response antworten. Die gültige Response muss folgendes Element enthalten:

- HTTP-Status-Code („4xx“)

Beispiel für eine gültige HTTP-Response:

```
HTTP/1.1 400 Bad request
```

3.2.2.4 HTTP-Body

Im HTTP-Body werden die in XML repräsentierten Container- bzw. Objekt-Informationen CMS-verschlüsselt übertragen.

Für die Prüfung werden Positiv- und Negativtestfallketten erstellt. Diese setzten sich aus verschiedenen Positiv- bzw. Negativtestfällen aus folgenden Kapiteln zusammen:

- HTTP-Verben
- HTTP-Header-Felder
- HTTP-Status-Codes
- CMS Inhaltsdatensicherung
- XML Transfersyntax für COSEM Objekte

3.2.2.5 HTTP-Status-Codes

Die technische Richtlinie [BSI TR-03109-1/AII] gibt vor, welche HTTP-Status-Codes verwendet werden **dürfen**. Das korrekte Verhalten wird durch Positiv- und Negativtestfälle getestet. Dazu werden gültige bzw. ungültige Requests an den Endpunkt des Webservice-Anbieter s gesendet. Dieser muss mit einer gültigen Response antworten.

Beispiel für einen gültigen HTTP-Request und eine gültige HTTP-Response:

```
GET https://ebsi0012345678.sm.bsi.bund.de:14059
/smgw/cosem/ldevs/ebsi0a12345678.sm/objects/3-
0100010801ff/attributes/1 HTTP/1.1
Host: ebsi0012345678.sm.bsi.bund.de:14059
Content-Length: 100
HTTP/1.1 200 OK
```

Beispiel für einen ungültigen HTTP-Request und eine gültigen HTTP-Response :

```
GET https://ebsi0012345678.sm.bsi.bund.de:14059
/smgw/cosem/ldevs/ebsi0a12345678.sm/objects/ [nicht vorhandenes
Objekt] /attributes/1 HTTP/1.1
Host: ebsi0012345678.sm.bsi.bund.de:14059
Content-Length: 100
HTTP/1.1 404 Not Found
```

3.2.2.6 HTTP-Version

Die Technische Richtlinie [BSI TR-03109-1] gibt vor, dass für den Transport der Nachrichten HTTP in der Version 1.1 genutzt werden **muss**.

Um dies zu testen, werden Positivtestfälle mit einem gültigen Request und Negativtestfälle mit einem nicht gültigen Request an den Endpunkt des Webservice-Anbieters gesendet.

Beispiel für einen gültigen HTTP-Request:

```
GET https://ebsi0012345678.sm.bsi.bund.de:14059
/smgw/cosem/ldevs/ebsi0a12345678.sm/objects/3-
0100010801ff/attributes/1 HTTP/1.1
Host: ebsi0012345678.sm.bsi.bund.de:14059
Content-Length: 100
```

Beispiel für einen nicht gültigen HTTP-Request:

```
GET https://ebsi0012345678.sm.bsi.bund.de:14059
/smgw/cosem/ldevs/ebsi0a12345678.sm/objects/3-
0100010801ff/attributes/1 HTTP/1.0
Host: ebsi0012345678.sm.bsi.bund.de:14059
Content-Length: 100
```

Der Webservice-Anbieter muss mit einer gültigen Response antworten. Die gültige Response muss folgende Elemente enthalten:

- HTTP-Status-Code („200“ bzw. „505“)
- HTTP-Header (optional und vom Dienst/Request abhängig)
- HTTP-Body (optional, abhängig vom Dienst)

Zwei Beispiele für eine gültige HTTP-Response:

Beispiel 1

```
HTTP/1.1 200 OK
```

```
Content-Type: application/vnd.de-dke-k461-cosem +xml;encap=cms-
tr03109
Content-Encoding: deflate
Content-Length: 2000
<CMS encoded and signed body>
```

Beispiel 2

```
HTTP/1.1 505 HTTP Version not supported
```

3.2.2.7 Testeingangskriterien, Abhängigkeiten

Bevor die Prüfung des HTTP-Protokolls erfolgen kann, muss die Prüfung des TLS-Protokolls und des SecMod erfolgreich abgeschlossen worden sein.

3.2.2.8 Testdaten

Für die Tests des HTTP-Protokolls müssen im SMGW verschiedene Logische Geräte (Logical Devices wie Zähler, Nutzer etc.) vorhanden sein. Die im HTTP-Body gesendeten Daten müssen den Schemata [XSD-COD] und [XSD-COR] entsprechen und mittels CMS verschlüsselt und signiert sein.

3.2.2.9 Hinweise zu möglichen Testwerkzeugen (informativ)

Für den Test können zum Beispiel folgende Tools eingesetzt werden:

- Smartbear SoapUI
- Parasoft SOAtest
- The Measurement Factory Co-Advisor

3.2.3 RESTful COSEM Webservices

Die technische Richtlinie [BSI TR-03109-1] gibt vor, dass die Kommunikationsszenarien und die darauf aufsetzenden Dienste und Anwendungsfälle mit Hilfe von RESTful Webservices im SMGW, beim SMGW Administrator und beim EMT erbracht werden **müssen**.

RESTful Webservices setzen auf HTTP auf. Durch die Tests der HTTP Verben , der HTTP Header Felder, des HTTP Body, der HTTP-Status-Codes und der HTTP Version wird implizit die korrekte Implementierung der RESTful Webservices mittels HTTP getestet. Auf einen expliziten Test kann verzichtet werden, da kein anderes Verhalten zu erwarten ist.

Die technische Richtlinie [BSI TR-03109-1/AII] macht für die Implementierung von RESTful Webservices in den folgenden Punkten weitere Vorgaben. Diese werden nicht über andere Protokolltests abgedeckt und müssen dementsprechend explizit getestet werden:

- Nachrichtenaustauschmuster Request-Response
- Längenbeschränkung der Request-URI
- HTTP Pipelining
- Response Timeout
- synchrone und asynchrone Kommunikation
- Aufrechterhaltung der Verbindung

- Query-Parameter
- Listen-Ressourcen
- Dynamisches Anlegen/Löschen von Ressourcen
- Fragmentierung von Inhaltsdaten

Die Implementierung der RESTful Webservices ist entscheidende Voraussetzung für darauf mittelbar und unmittelbar aufbauende Anwendungsfälle. Um die Auswirkungen des gegenwärtigen Spezifikationsstandes auf die Formulierung der Testfälle in darüber liegenden OSI-Schichten für AP2 und AP3 hinreichend bewerten zu können, ist eine entsprechend detailliertere Betrachtung des aktuellen Anforderungsstandes in AP1 erfolgt.

3.2.3.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	A	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	C	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	ja	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	A	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	B	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 37: Bewertungskriterien für WAN / RESTful COSEM Webservices

3.2.3.2 Nachrichtenaustauschmuster Request-Response

Die Kommunikation erfolgt zwischen Webservice-Benutzer und Webservice-Anbieter. Der Webservice-Benutzer sendet einen Request an den Webservice-Anbieter, dieser antwortet mit einer Response. Als Nachrichtenaustauschmuster wird Request-Response genutzt, das bedeutet, dass es keine Response ohne Request geben darf. Um dies zu testen, werden Negativtestfälle durchgeführt. Auf die Durchführung von Positivtestfällen kann verzichtet werden, da die Prüfung auf korrektes Verhalten implizit in den Anwendungsfalltests des WAN erfolgt.

In den Negativtestfällen werden gültige Responses ohne Bezug zu einem Request vom SMGW Administrator an das SMGW gesendet, diese Response muss ignoriert werden.[33]

3.2.3.3 Längenbeschränkung der Request-URI

Die Request-URI soll nach [BSI TR-03109-1/AII] nicht länger als 4000 Zeichen lang sein. Eine Request-URI kann wie folgt aussehen:

```
https://ebsi0012345678.sm.bsi.bund.de:14059
/smgw/cosem/ldevs/ebsi0a12345678.sm/objects/3-0100010801ff/attributes/1
```

Die Länge der Request-URI ist hauptsächlich durch die verwendete Domain (im Beispiel: `sm.bsi.bund.de`) bestimmt, da die Längen der anderen Teile des Aufrufs nur gering variieren. In [BSI TR-03109-1/AII] wird die Begrenzung der Länge der Request-URI empfohlen, es kann aber im begründeten Fall abgewichen werden. Weiterhin macht HTTP keine Vorgaben zur maximalen Länge einer Request-URI. Durch die Tests der HTTP Verben und der WAN-Anwendungsfälle wird implizit getestet, dass Request-URIs mit einer Länge kleiner 4000 Zeichen korrekt verarbeitet werden. Da das SMGW eine Request-URI mit 4000 Zeichen verarbeiten können muss, wird ein Positivtestfall erstellt.

In dem Positivtestfall sendet der Webservice-Benutzer einen gültigen Request mit einer 4000 Zeichen langen Request-URI an den Webservice-Anbieter, dieser muss die Anfrage verarbeiten und mit einem gültigen HTTP-Status-Code antworten.

3.2.3.4 HTTP-Pipelining

Es darf laut technischer Richtlinie [BSI TR-03109-1/AII] innerhalb einer HTTP-Session erst ein neuer Request `n` versendet werden, wenn zu dem vorher gesendeten Request `n-1` eine Response vorliegt. Um dies zu testen, werden Positiv- und Negativtestfälle durchgeführt.[34]

In den Positivtestfällen werden innerhalb einer HTTP-Session gültige Requests vom Webservice-Benutzer an den Webservice-Anbieter gesendet, dieser muss jeweils mit einer gültigen Response antworten. Ein neuer Request darf erst gesendet werden, wenn zu dem vorhergehenden Request eine Response empfangen wurde. Um eine möglichst enge zeitliche Aneinanderreihung (neuer Request folgt direkt auf eine Response) von Requests zu ermöglichen, kann nur die Strecke SMGW Administrator (Webservice-Benutzer) → SMGW (Webservice-Anbieter) betrachtet werden.

Bei den Negativtestfällen werden gültige Requests in enger zeitlicher Abfolge innerhalb einer HTTP-Session vom Webservice-Benutzer an den Webservice-Anbieter gesendet, bevor eine Response vom Webservice-Anbieter an den Webservice-Benutzer gesendet wurde. Der Webservice-Anbieter darf nur den ersten Request verarbeiten, alle weiteren Requests müssen ignoriert werden.[35] Auch bei den Negativtestfällen kann nur die Strecke SMGW Administrator (Webservice-Benutzer) → SMGW (Webservice-Anbieter) betrachtet werden.

3.2.3.5 Response-Timeout

Der Webservice-Anbieter muss einen Response-Timeout nach [BSI TR-03109-1/AII] konfigurieren können[36]. Trifft innerhalb der Timeoutzeit keine Response beim Webservice-Benutzer ein, wird die HTTP-

33 Das konkrete Verhalten wäre durch den Herausgeber der TR ggf. noch zu definieren.

34 Es wird angenommen, dass die Netzwerk-Latenz an der WAN-Schnittstelle im Feldeinsatz keine Rolle spielen wird, da entsprechend leistungsfähige Verbindungen verfügbar sind – wenngleich die TR hier keine Vorgaben macht. Schmalbandige Verbindungen würden hier ein sehr langsames Systemverhalten verursachen, da stets auf Antworten zu warten wäre, bevor die nächste Aktion möglich ist.

35 vgl. 33

36 Die Stelle, an der die Konfiguration vorzunehmen ist, wäre vom TR-Herausgeber noch zu definieren.

Session und die Transportverbindung von beiden Seiten getrennt. Um dies zu testen, werden Positivtestfälle durchgeführt.

In den Positivtestfällen sendet der Webservice-Benutzer einen gültigen Request an den Webservice-Anbieter, dieser darf nicht innerhalb der konfigurierten Timeoutzeit antworten. Daraufhin muss die HTTP-Session und die Transportverbindung von beiden Seiten getrennt werden. Die folgenden Webservice-Benutzer - Webservice-Anbieter Kombinationen sind möglich:

Webservice-Benutzer	**Webservice-Anbieter**
SMGW	SMGW Administrator
SMGW	EMT

Tabelle 38: Webservice-Benutzer - Webservice-Anbieter Kombinationen, Testobjekt in *kursiv*

Bei diesen Kombinationen sind die im SMGW eingestellten Timeoutzeiten nicht relevant, da ein Webservice-Anbieter hier keine Antwort sendet. Das SMGW muss dann die Trennung initialisieren. Die Kombination SMGW Administrator/SMGW kann nicht sinnvoll getestet werden, da die Erzeugung eines Timeouts beim SMGW nicht bzw. nur sehr schwer herbeizuführen ist.

3.2.3.6 Synchrone und asynchrone Kommunikation

Wenn der Webservice-Anbieter innerhalb der Timeoutzeit keine synchrone Antwort an den Webservice-Benutzer senden kann, sendet der Webservice-Anbieter eine synchrone Response mit einem entsprechenden HTTP-Status-Code und ggf. später eine asynchrone Response mit den entsprechend angefragten Daten. Um dies zu testen, werden Positivtestfälle durchgeführt.

In den Positivtestfällen werden gültige Requests vom Webservice-Benutzer an den Webservice-Anbieter gesendet. Da der Webservice-Anbieter innerhalb der Timeoutzeit keine entsprechende Response senden kann, sendet er nur einen HTTP-Status-Code („408“-Fehlermeldung bzw. „202“-Asynchrone Antwort). Der HTTP-Status-Code „408“ signalisiert, dass der Request nicht in der vorgegebenen Zeit bearbeitet werden konnte und zu einem späteren Zeitpunkt erneut an den Webservice-Anbieter gesendet werden muss. Beim HTTP-Status-Code „202“ wird später asynchron eine Response mittels POST an die im Request-Header-Feld „x-ContactURI“ angegebene URI gesendet. Weiterhin muss im Request das Header-Feld „x-CID“ vorhanden sein, um eine Zuordnung der Response zum Request zu ermöglichen. Bei der asynchronen Kommunikation agiert der Webservice-Anbieter als Webservice-Benutzer und der Webservice-Benutzer als Webservice-Anbieter.

Mögliche Webservice-Benutzer - Webservice-Anbieter Kombinationen für die Tests sind in folgender Tabelle dargestellt:

Webservice-Benutzer	**Webservice-Anbieter**
SMGW	SMGW Administrator
SMGW	EMT

Tabelle 39: Webservice-Benutzer - Webservice-Anbieter Kombinationen, Testobjekt in *kursiv*

Die Kombination SMGW Administrator/SMGW kann nicht sinnvoll getestet werden, da die Erzeugung eines Timeouts beim SMGW nicht bzw. nur sehr schwer herbeizuführen ist. Die beiden in der Tabelle aufgeführten Kombinationen können hingegen problemlos getestet werden, da man das Verhalten des Webservice-Anbieters (HTTP-Status-Code, asynchrone Response) direkt beeinflussen kann.

3.2.3.7 Aufrechterhaltung der Verbindung

HTTP unterstützt in der Version 1.1 [RFC2616] die Aufrechterhaltung der Verbindung nach einer Response. Der Webservice-Benutzer kann innerhalb der gleichen HTTP-Session somit mehrere Requests an den

Webservice-Anbieter senden und muss nicht bei jedem Request eine neue Verbindung aufbauen. Wird im HTTP-Header das Feld „Connection“ nicht angegeben, muss davon ausgegangen werden, dass die Verbindung persistent ist. Ein Verbindungsabbau nach dem Empfang der Response kann über die Angabe des HTTP-Header-Feldes „Connection“ mit dem Wert „close“ signalisiert werden. Um dies zu testen werden Positivtestfälle durchgeführt.

In den Positivtestfällen werden gültige Requests vom Webservice-Benutzer an den Webservice-Anbieter gesendet. Agiert der SMGW Administrator als Webservice-Benutzer (erste Kombination, Tabelle 40) , muss im Request zusätzlich das Header-Feld „Connection“ mit dem Wert „close“ enthalten sein. Damit kann getestet werden, dass der vom Webservice-Benutzer signalisierte Verbindungsabbau nach Empfang der Response stattfindet. Agiert das SMGW als Webservice-Benutzer (zweite und dritte Kombination, Tabelle 40), kann nicht sichergestellt werden, dass im HTTP-Header des Request das Feld „Connection“ mit dem Wert „close“ gesetzt ist. Aus diesem Grund muss der Webservice-Anbieter (SMGW Administrator bzw. EMT) im Response-Header das Feld „Connection“ mit dem Wert „close“ angeben. Dadurch wird getestet, dass der vom Webservice-Anbieter signalisierte Verbindungsabbau stattfindet.

Webservice-Benutzer	**Webservice-Anbieter**
SMGW Administrator	*SMGW*
SMGW	SMGW Administrator
SMGW	EMT

Tabelle 40: Webservice-Benutzer - Webservice-Anbieter Kombinationen, Testobjekt in *kursiv*

3.2.3.8 Query-Parameter

Laut der technischen Richtlinie [BSI TR-03109-1/AII] können Query-Parameter an die Request-URI angehängt werden. Damit kann das Ergebnis gefiltert und die zu übertragende Datenmenge reduziert werden. Die Query-Parameter werden in folgender Form angegeben:

```
<Request-URI> ?parameter1=wert1 &parameter2=wert2&...
```

Die Einleitung der Query-Parameter beginnt mit „?“, mehrere Query-Parameter werden mittels „&“ verknüpft. Wird der gleiche Parameter mehrfach angegeben, gilt der Wert seines ersten Auftretens und alle weiteren Werte müssen ignoriert werden. Weiterhin müssen Query-Parameter für die Dienste Delete, Create und Action ignoriert werden, für den Dienst Set sollen keine Query-Parameter angegeben werden. Für den Dienst Get können Query-Parameter angegeben werden. Der Zugriff kann selektiv auf Inhalte von COSEM-Attributen erfolgen oder mittels universellen Query-Parametern. Um das Verhalten zu testen, werden Positiv- und Negativtestfälle durchgeführt.

In den Positivtestfällen werden gültige Requests mit 1-n Query-Parametern für den Dienst Get an den Webservice-Anbieter gesendet. Der Zugriff erfolgt dabei sowohl selektiv auf Inhalte von COSEM-Attributen als auch über universelle Query-Parameter. Der Webservice-Anbieter muss mit einer gültigen Response antworten. In der Response dürfen nur die per Query-Parameter angeforderten Werte vorhanden sein.

Die möglichen Parameter für den selektiven Zugriff und die universellen Query-Parameter sind in den folgenden beiden Tabellen aufgeführt:

Query-Parameter	Bedeutung	Wert	Standardwert
sa.fromidx	gibt den Index des ersten Array Eintrages bei Zugriffen auf COSEM-Array-Attribute an	Integer, 1...n (dezimal) oder hex (x)	1
sa.count	limitiert die Zahl der zu übertragenden Einträge bei Get	Integer, 1...n (dezimal) oder hex	leer: unlimitiert
sa.toidx	gibt den Index des letzten Eintrages bei Zugriffen auf das adressierte COSEM-Array-Attribute an	Integer, 1...n (dezimal) oder hex	leer: letzter Eintrag
sa.fromcol	gibt die erste Spalte an, die ausgelesen werden soll	0,1...n	leer: erste Spalte
sa.tocol	gibt die letzte Spalte an, die ausgelesen werden soll	0,1...n	leer: letzte Spalte
sa.retrievecolumns	enthält Liste von Deskriptoren die zur Spaltenauswahl dienen	Descriptor, {Descriptor}	leer: alle Spalten
sa.filtercolumn	enthält den Deskriptor der Spalte auf den die Wertauswahl angewandt wird	Descriptor	
sa.from	liefert nur Werte die größer oder gleich (sa.from) sind.	Type: value	leer: niedrigster Wert
sa.to	liefert nur Werte die kleiner oder gleich (sa.to) sind.	Type: value	leer: höchster Wert

Tabelle 41: Parameter und Werte für den selektiven Zugriff

873

Query-Parameter	Bedeutung	Ressource	Wert	Standardwert
`q.fromidx`	gibt den Index beim Zugriff auf eine Listen-Ressource an	Listen	`1...n (dezimal), hex (x)`	1
`q.count`	limitiert die Zahl der zu übertragenden Einträge bei einer Liste	`1...n (dezimal), hex(x)`	Listen	leer: unlimitiert
`q.depth`	legt die Tiefe der Ausgelesen Datenstruktur fest	`0..n (dezimal), hex (x)` `0`: nur das Listen-Element selbst mit Attributen wird geliefert.	alle	URI mit trailing /: 1 URI ohne trailing /: unlimited
`q.fromtime`	Filter auf Listen mit Zeitangabe: qb dieser Zeit	ISO8601	Listen	kein Limit nach unten
`q.totime`	Filter auf Listen mit Zeitangabe: bis zu dieser Zeit	ISO8601	Listen	kein Limit nach oben

Tabelle 42: Universelle Query-Parameter

Weiterhin wird mittels Positivtestfällen geprüft, dass Query-Parameter bei den Diensten Delete, Create und Action ignoriert werden.

In den Negativtestfällen werden für den Dienst Get in der Request-URI nicht definierte Query-Parameter angegeben bzw. Werte außerhalb des Wertebereichs verwendet.[37]

3.2.3.9 Listen-Ressourcen

Der URI-Baum enthält nach [BSI TR-03109-1/AII] folgende Listen-Ressourcen :

- ldevs
- objects
- containers
- attributes
- methods

Die Elemente einer Listen-Ressource können über einen GET-Request abgefragt werden, Listen-Ressourcen können leer sein. Zur Filterung können folgende Query-Parameter verwendet werden:

- q.fromidx – listet die Elemente ab dem angegebenen Index auf
- q.count – liefert die Anzahl der Elemente einer Liste zurück
- q.depth – legt fest die Tiefe der zurückgelieferten Element-Strukturen fest, q.depth=0 liefert nur die Listen-Ressource ohne Unterelemente zurück

37 Das konkrete Verhalten, welches vom Webservice-Anbieter gefordert wird, wäre durch den TR-Herausgeber noch festzulegen.

Über das Attribut „count“ in der angefragten Listen-Ressource wird mitgeteilt, wie viele Unterelemente zurückgeliefert wurden. Es werden Positivtestfälle durchgeführt.

In den Positivtestfällen werden gültige GET-Requests für die unterschiedlichen Listen-Ressourcen mit und ohne den möglichen Query-Parametern an den Webservice-Anbieter geschickt. Dieser muss mit einer gültigen Response antworten.

3.2.3.10 Dynamisches Anlegen/Löschen von Ressourcen (Containern, Objekten)

Ressourcen können mit Hilfe der beiden HTTP-Verben PUT und DELETE angelegt bzw. gelöscht werden. Gibt man in einer Request-URI eine Ressource an, die noch nicht existiert, wird diese durch PUT neu angelegt. Die entsprechenden Objektdaten müssen im HTTP-Body mitgegeben werden. Wird in der Request-URI eine existierende Ressource angegeben, wird diese überschrieben. Weiterhin ist nicht vorgesehen, dass eine Ressource mit Hilfe von POST anlegt werden kann. Um eine Ressource zu löschen muss in der Request-URI nur die entsprechende Ressource angegeben werden. Um das Verhalten zu testen, werden Positiv- und Negativtestfälle durchgeführt.

In den Positivtestfällen sendet der Webservice-Benutzer gültige PUT- und DELETE-Requests an den Webservice-Anbieter. Der Webservice-Anbieter muss daraufhin neue Ressourcen anlegen bzw. vorhandene Ressourcen löschen. Weiterhin muss der Webservice-Anbieter die erfolgreiche Anlage bzw. Löschung einer Ressource mit dem HTTP-Status-Code „201“ (Anlage) bzw. „204“ (Löschung) beantworten.

Bei den Negativtestfällen werden ungültige POST- und DELETE-Requests vom Webservice-Benutzer an den Webservice-Anbieter gesendet. Der Webservice-Anbieter muss die ungültigen Requests mit dem HTTP-Status-Code „404“ (Ressource nicht gefunden) bzw. „405“ (HTTP-Methode nicht zulässig) abweisen.

3.2.3.11 Fragmentierung von Inhaltsdaten

Um große Datenmengen transferieren zu können, können die Daten in Blöcke aufgeteilt und mittels Blocktransfer übertragen werden. Zulässig ist diese Form der Übertragung nur für die idempotenten Operationen GET und PUT. Erst wenn alle Blöcke übertragen sind, gilt die Operation als abgeschlossen. Um Daten mittels Blocktransfer zu übertragen, muss im HTTP-Header des Requests das Feld „Range“ mit der entsprechen Anzahl der zu übertragenden Bytes angegeben sein. Um das Verhalten zu testen, werden Positiv- und Negativtestfälle durchgeführt.

In den Positivtestfällen sendet der Webservice-Benutzer gültige PUT- und GET-Requests an den Webservice-Anbieter. Der Webservice-Anbieter muss daraufhin die zu übertragenden Daten in Blöcke aufteilen und übermitteln. Pro Block gibt es eine Response. Jede Response muss den HTTP-Status-Code „206“ und die HTTP-Header-Felder „Content-Range“ und „Content-Length“ haben.

Bei den Negativtestfällen werden ungültige Requests vom Webservice-Benutzer an den Webservice-Anbieter gesendet. Der Webservice-Anbieter muss die ungültigen Requests mit dem HTTP-Status-Code „416“ (angegebene Range passt nicht zur Ressource) bzw. „4xx “ abweisen.

3.2.3.12 Zugriffsrechte

Mit der Authentifizierung über TLS wird festgelegt, welche Zugriffsrechte der Webservice-Benutzer auf die Ressourcen des Webservice-Anbieters hat. Generell darf der Webservice-Benutzer nur mittels der HTTP-Verben GET, PUT, POST und DELETE auf den Webservice-Anbieter zugreifen. Werden Ressourcen vom Webservice-Benutzer angefragt, auf die er keinen Zugriff haben darf, muss der Webservice-Anbieter mit dem HTTP-Status-Code „404“ antworten. Um das Verhalten zu testen, werden Positiv- und Negativtestfälle durchgeführt.

In den Positivtestfällen werden gültige Requests vom Webservice-Benutzer an den Webservice-Anbieter gesendet. Dieser muss mit einer gültigen Response antworten.

Bei den Negativtestfällen werden ungültige Requests (z. B. andere HTTP-Verben wie PATCH, HEAD, ...) vom Webservice-Benutzer an den Webservice-Anbieter gesendet. Der Webservice-Anbieter muss die ungültigen Requests mit einer Fehlermeldung abweisen.

3.2.3.13 Testeingangskriterien, Abhängigkeiten

Bevor die Tests des RESTful COSEM Webservices erfolgen können, müssen die Tests für HTTP, TLS und für das SecMod abgeschlossen sein.

3.2.3.14 Testdaten

Für die Tests der RESTful COSEM Webservices müssen im SMGW verschiedene Logische Geräte (Logical Devices wie Zähler, Nutzer etc.) vorhanden sein. Die im HTTP-Body gesendeten Daten müssen den Schemata [XSD-COD] und [XSD-COR] entsprechen und mittels CMS verschlüsselt und signiert sein.

3.2.3.15 Hinweise zu möglichen Testwerkzeugen (informativ)

Für den Test können zum Beispiel folgende Tools eingesetzt werden:

- Smartbear SoapUI
- Parasoft SOAtest

3.2.4 CMS Inhaltsdatensicherung

Die Übertragung von Daten (COSEM Objekte/Objekt-Container/ Objekt-Attribute im HTTP-Body) zwischen dem SMGW und EMT kann über Dritte (z. B. SMGW-Admin) erfolgen. Deshalb besteht laut [BSI TR-03109-1] die Notwendigkeit, dass die zu übertragenden Daten nicht nur in einem gesicherten TLS-Kanal übertragen werden, sondern auch inhaltsverschlüsselt sein müssen. Die [BSI TR-03109-1] sieht dafür das CMS-Format gemäß [RFC5652] und [RFC5083] vor. Damit wird sichergestellt, dass Dritte, bei denen eine TLS-Verbindung terminiert wird (z. B. SMGW-Admin) und ein neuer TLS-Kanal zum EMT aufgebaut wird, die Daten nicht im Klartext einsehen können. Durch die Nutzung des CMS-Formats werden die Inhaltsdaten innerhalb der TLS-Verbindung ein weiteres Mal verschlüsselt und signiert. Somit kann der EMT sicherstellen, dass die empfangenen Daten nicht manipuliert oder im Klartext eingesehen werden konnten.

[BSI TR-03109-1/AI] beschreibt den Aufbau der CMS-gesicherten Pakete (Datenfelder und deren erlaubter Inhalt) und macht Vorgaben, welche kryptografischen Verfahren für die Verschlüsselung und Signatur eingesetzt werden sollen.

962 3.2.4.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	Die geforderte Funktionalität impliziert entsprechende Interoperabilität auf der betrachteten OSI-Schicht.
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	ja	Aufsetzend auf etablierten Standards.
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	B	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	B	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 43: Bewertungskriterien für WAN / CMS Inhaltsdatensicherung

963 3.2.4.2 Anforderungen der TR

964 Nachfolgende Anforderungen stellt die TR explizit an die Implementierung der CMS Inhaltsdatensicherung.

ID	Anforderung (abstrakt)	Konkretisierung [BSI TR-03109-1], [BSI TR-03109-1/AI]	Zusätzliche Referenz(en)
	Übergreifende Anforderung	*Anforderung*	*Anforderungsquelle*
WAN.CMS.01	Zur Sicherung der Inhaltsdaten im WAN MÜSSEN gemäß [GW_PP] die COSEM Objekte bzw. aggregierten Objekt-Container für den Endempfänger verschlüsselt und vom Absender signiert werden.	-	[BSI TR-03109-1]
WAN.CMS.01.01	WAN.CMS.01	Für die Kennzeichnung der COSEM-Daten mit XML-Transfersyntax und CMS Inhaltsdatensicherung MUSS der Content-Type `application/vnd.de-dke-k461-cosem+xml;encap=cms-tr03109` verwendet werden.	[BSI TR-03109-1]
WAN.CMS.01.02	WAN.CMS.01	Für die Kennzeichnung der CMS-Inhaltsdatenverschlüsselung ohne vorherige Kompression der XML Daten DARF KEIN Content-Encoding Header Feld vorhanden sein.	[BSI TR-03109-1]
WAN.CMS.01.03	WAN.CMS.01	Für die Kennzeichnung der CMS-Inhaltsdatenverschlüsselung mit vorheriger Kompression der XML Daten MUSS das Content-Encoding `deflate` verwendet werden.	[BSI TR-03109-1]
WAN.CMS.01.04	WAN.CMS.01	Server und Client MÜSSEN sowohl komprimierte als auch unkomprimierte CMS-Daten verarbeiten können. Der ASN.1 ContentType des verschlüsselten Inhalts hat den ASN.1-Object Identifier-Wert „`id-data`“ oder „`id-ct-compressedData`“.	[BSI TR-03109-1]
WAN.CMS.01.05	WAN.CMS.01	Requests/Reponses ohne HTTP-Body DÜRFEN NICHT mittels Inhaltsdatensicherung abgesichert werden, d.h. Status-Codes über den HTTP-Header werden durch TLS gesichert, aber nicht zusätzlich CMS-verpackt.	-
WAN.CMS.02	Es soll Authenticated-Enveloped-Data genutzt werden	Die Datenstruktur `AuthEnvelopedData` aus [BSI TR-03109-1/AI] soll verwendet werden	[BSI TR-03109-1/AI]

ID	Anforderung (abstrakt)	Konkretisierung [BSI TR-03109-1], [BSI TR-03109-1/AI]	Zusätzliche Referenz(en)
	Übergreifende Anforderung	*Anforderung*	*Anforderungsquelle*

WAN.CMS.02.01	WAN.CMS.02	Es sollen folgende OIDs verwendet werden:
		
		`ecka-eg-X963KDF-SHA256 OBJECT IDENTIFIER ::= {ecka-eg ecka-eg-x963KDF(1) 3}`
		
		`ecka-eg-X963KDF-SHA384 OBJECT IDENTIFIER ::= {ecka-eg ecka-eg-x963KDF(1) 4}`
		
		`ecka-eg-X963KDF-SHA512 OBJECT IDENTIFIER ::= {ecka-eg ecka-eg-x963KDF(1) 5}`
			[BSI TR-03109-1/AI]

WAN.CMS.02.02	WAN.CMS.02	Für die Key Encryption sollen die Algorithmen `id-aes128-wrap`, `id-aes192-wrap`, `id-aes256-wrap` verwendet werden. Das Parameter-Feld bleibt bei diesen Algorithmen leer	[BSI TR-03109-1/AI]
WAN.CMS.02.03	AES im GCM-Mode für die authentisierte Content-Encryption	• Algorithmen mit den OIDs `id-aes128-gcm`, `id-aes192-gcm`, `id-aes256-gcm` sollen unterstützt werden • Bei Verwendung einer dieser OIDs ist im Feld `encryptedKey` der mit dem gewählten Key-Encryption-Algorithmus verschlüsselte (zufällig erzeugte) Content-Encryption-Key *K* enthalten (AESxxx-Wrap(*K*)). • Der Content-Encryption-Key K für die Verschlüsselung und MAC-Sicherung der Daten muss stets unmittelbar vor seiner Verwendung zufällig erzeugt werden und darf jeweils nur für die Versendung einer Nachricht verwendet werden.	[BSI TR-03109-1/AI]

ID	Anforderung (abstrakt)	Konkretisierung [BSI TR-03109-1], [BSI TR-03109-1/AI]	Zusätzliche Referenz(en)
	Übergreifende Anforderung	*Anforderung*	*Anforderungsquelle*
WAN.CMS.02.04	AES im CBC-CMAC-Mode für die authentisierte Content-Encryption	• Die Verschlüsselung und MAC-Sicherung soll im CBC-CMAC-Mode via der Algorithmen `id-aes-CBC-CMAC-128, id-aes-CBC-CMAC-192, id-aes-CBC-CMAC-256` unterstützt werden. Die OIDs werden in Anhang A definiert. • Das parameters-Feld muss hier weggelassen werden, d.h. es gilt `IV=0`.und der MAC besteht aus 16 OCTETS. • Bei Verwendung einer dieser OIDs ist im Feld `encryptedKey` die mit dem gewählten Key-Encryption-Algorithmus verschlüsselte Konkatenation *Kenc||Kmac* enthalten (AESxxx-Wrap(*Kenc||Kmac*)). Hierbei ist *Kenc* der (zufällig erzeugte) Schlüssel für die Verschlüsselung des Inhalts mit AES im CBC-Mode und *Kmac* der (zufällig erzeugte) Schlüssel für die MAC-Sicherung mit AES im CMAC-Mode. • Die Schlüssel Kenc und Kmac für die Verschlüsselung und MAC-Sicherung der Daten müssen stets unmittelbar vor seiner Verwendung zufällig erzeugt werden und dürfen jeweils nur für die Versendung einer Nachricht verwendet werden.	[BSI TR-03109-1/AI]
WAN.CMS.03	Es soll die Datenstruktur Signed-Data genutzt werden	Das Profil aus [BSI TR-03109-1/AI] ab Seite 11 soll verwendet werden	[BSI TR-03109-1/AI]
WAN.CMS.03.01	WAN.CMS.03	Es sind die OIDs `id-sha-256, id-sha-384, id-sha-512` für die Berechnung des Message Digest zu unterstützen. Das Parameter-Feld bleibt leer.	[BSI TR-03109-1/AI]

ID	Anforderung (abstrakt)	Konkretisierung [BSI TR-03109-1], [BSI TR-03109-1/AI]	Zusätzliche Referenz(en)
	Übergreifende Anforderung	*Anforderung*	*Anforderungsquelle*

WAN.CMS.03.02	WAN.CMS.03	Es sollen die folgenden OIDs verwendet werden:
		`ecdsa-with-Sha-256 OBJECT IDENTIFIER ::= {id-ecSigType ecdsa-with-specified(3) 2}`
		
		`ecdsa-with-Sha-384 OBJECT IDENTIFIER ::= {id-ecSigType ecdsa-with-specified(3) 3}`
		
		`ecdsa-with-Sha-512 OBJECT IDENTIFIER ::= {id-ecSigType ecdsa-with-specified(3) 4}`
		
		Als Signatur-Algorithmus ist hierbei jeweils die OID zu verwenden, deren Suffix mit der Hash-Funktion übereinstimmt, welche im DigestAlgorithm-Feld der entsprechenden SignerInfos enthalten ist.
		
		Die Codierung der Signatur muss im X9.62 Format gemäß BSI TR-03111, Elliptic Curve Cryptography, Version 2.0, 2012 Kp. 5.2.2 erfolgen.
			[BSI TR-03109-1/AI]

Tabelle 44: Anforderungen WAN / CMS Inhaltsdatensicherung

3.2.4.3 Testdurchführung

Es werden die vorgesehenen dynamischen (3.2.4.3.1) Tests beschrieben.

3.2.4.3.1 Dynamische Tests

Nachfolgende Tabellen geben eine Übersicht über die vorzusehenden Tests zu den Interoperabilitäts-aspekten.

Anforderungs-referenz	Testfokus	Durchführung	Erwartetes Verhalten
WAN.CMS.01.01	Eingesetzter Content-Type	Analyse eines vom SMGW versendeten CMS-Datenpakets	Vom SMGW wird der Content-Type application/vnd.de-dke-k461-cosem+xml;encap=cms-tr03109 gesetzt
WAN.CMS.01.02	Content Encoding Header	Senden eines HTTP-Requests ohne Accept-Encoding Header	Response enthält kein Content-Encoding Header
WAN.CMS.01.03	Content Encoding Header	Senden eines HTTP-Requests mit Accept-Encoding Header	Response enthält Content-Encoding deflate
WAN.CMS.01.04	Komprimierte CMS Daten	Senden von komprimierten CMS Daten an das SMGW	Das SMGW verarbeitet die komprimierten Datan korrekt
WAN.CMS.01.05	Verhalten bei Reuests / Responses ohne HTTP-Body	Senden eines Requests / einer Response ohne HTTP-Body / Status-codes	Die Status-codes werden nicht mittels CMS gesichert.
WAN.CMS.02	Aufbau der Datenstruktur	Prüfung der einzelnen Parameterfelder des CMS-Datenpakets auf Konformität der in [BSI TR-03109-1/AI] geforderten Werte	Die Felder des Datenpakets beinhalten die geforderten Parameter
WAN.CMS.02.01	Überprüfung der verwendeten OIDs	Entschlüsseln des CMS-Datencontainers	Es ist möglich mit den angegebenen OIDs den Klartext empfängerseitig wiederherzustellen
WAN.CMS.02.02	Überprüfung der Key Encryption Algorithmen	Schlüssel, die vom SMGW mit CMS verschlüsselt wurden entschlüsseln	Die Schlüssel können mit den vorgegebenen Algorithmen wiederhergestellt werden
WAN.CMS.02.03	AES im GCM-Mode für die Content Encryption	• Prüfung auf eingesetzte Algorithmen • Mehrere Kenc und Kmac Schlüssel aus CMS-gesicherten Nachrichten analysieren	• Es werden seitens des SMGW die geforderten Algorithmen unterstützt • Es wird bei ausreichender Anzahl von analysierten Nachrichten keine Doppelung von Schlüsseln festgestellt
WAN.CMS.02.04	AES im CBC-CMAC-Mode für die Content Encryption	• Prüfung auf eingesetzte Algorithmen • Prüfung auf nicht vorhandenes parameters-Feld • Mehrere Kenc und Kmac Schlüssel aus CMS-gesicherten Nachrichten analysieren	• Es werden seitens des SMGW die geforderten Algorithmen unterstützt • paramters-Feld ist nicht vorhanden • Es wird bei ausreichender Anzahl von analysierten Nachrichten keine Doppelung von Schlüsseln festgestellt

WAN.CMS.03	Aufbau der Datenstruktur	Prüfung der einzelnen Parameterfelder des CMS-Datenpakets auf Konformität der in [BSI TR-03109-1/AI] geforderten Werte	Die Felder des Datenpakets beinhalten die geforderten Parameter
WAN.CMS.03.01	Berechnung des Message Digest	Berechnung des Message Digest mit den geforderten Algorithemn	Message Digest kann mit einem der geforderten Algorithmen berechnet werden
WAN.CMS.03.02	Überprüfung der verwendeten OIDs der Signatur	• Prüfung der Signatur • Abgleich des Signatur-Algorithmus, welcher im DigestAlgorithm-Feld angegeben ist. • Prüfung des Codierungsformats	• Signatur kann erfolgreich verifiziert werden • Das Codierungsformat stimmt mit dem geforderten überein

Tabelle 45: Testdurchführung – Interoperabilität: Anbindung

970 3.2.4.4 Testeingangskriterien, Abhängigkeiten

971 Nachfolgende Tabelle gibt eine Übersicht über die Anforderungen an eine Testumgebung

Umgebungsan-forderung	**Umzusetzender Standard**	**Implementierungsmöglichkeiten**
Bereitstellung SecMod	[BSI TR-03109-2]	Zu beachten: grundsätzlich ist das SecMod im SMGW implementiert. Testvoraussetzung ist neben dem erfolgreichen Bestehen der CC-Evaluierung auch der erfolgreich abgeschlossene Konformitätstest [BSI TR-03109-2]. Für die Tests [BSI TR-03109-TS-1] agiert das SecMod auch als Teil der Testumgebung.
TLS	[BSI TR-03109-1]	-
HTTP	[BSI TR-03109-1]	-
COSEM	[BSI TR-03109-1/AII]	-
Anwendungsdaten	[BSI TR-03109-1]	-
WAN-Schnittstelle	[BSI TR-03109-1]	-

Tabelle 46: Testumgebungsanforderungen

3.2.4.5 Testdaten

Testdaten-forderung	Umzusetzender Standard	Anforderung TR	Hinweise
Anwendungsdaten	entsprechende Standards des darüberliegenden Protokolls		Es werden Anwendungsdaten benötigt, die mit verschiedenen zugelassenen und nicht zugelassenen Cipher-Suites verschlüsselt wurden. Die im HTTP-Body gesendeten Daten müssen den Schemata [XSD-COD] und [XSD-COR] für Positivtestfälle entsprechen und für Negativtests von ihnen abweichen.

Tabelle 47: Testdatenanforderungen

3.2.4.6 Hinweise zu möglichen Testwerkzeugen (informativ)

-

3.2.5 XML Transfersyntax für COSEM Objekte

Für diesen Abschnitt erwartet das BSI Änderungen an den Bezugsdokumenten. Aus Sicht der Konzeptautoren ist die abstrakte Beschreibung jedoch hinreichend und für den gewählten Testansatz auch erforderlich. Ggf. sind im Rahmen folgender Projektarbeitspakete Anpassungen erforderlich.

In der technischen Richtlinie [BSI TR-03109-1/AII] werden Vorgaben zu den folgenden Punkten für die XML Transfersyntax gemacht :

- XML Inhaltskodierung
- XSD Schema Relation
- URI Resource-Tree

981 3.2.5.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	A	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	C	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	ja	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	A	-
	Informativ: bekannte Sicherheits-risiken und Angriffsszenarien	Auswahl (ja oder nein)	ja	Angriffe auf XML-Parser sind bekannt
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	C	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 48: Bewertungskriterien für WAN / XML Transfersyntax für COSEM Objekte

982 3.2.5.2 XML Inhaltskodierung

983 Der im HTTP-Body übertragene XML-Inhalt muss in UTF-8 kodiert sein. Dazu muss die erste Zeile im XML-
984 Inhalt wie folgt aussehen:

985 `<?xml version="1.0" encoding="UTF-8"?>`

986 Die weiteren Daten müssen im XML-Inhalt in UTF-8 kodiert sein. Auf die Durchführung von Positiv- und
987 Negativtestfällen kann verzichtet werden, da die Prüfung auf korrekte bzw. fehlerhafte Inhaltskodierung in
988 den Anwendungsfalltests des WAN erfolgt.

989 3.2.5.3 XSD Schema Relation

990 Die im HTTP-Body übertragenen Daten und XML-Strukturen müssen valide zu den Schemata [XSD-COD]
991 und [XSD-COR] sein. Dafür müssen folgende Punkte getestet werden:

992 • der XML-Inhalt muss wohlgeformt sein

993 • es muss einen Verweis auf die Schemata [XSD-COD] und [XSD-COR] geben

994 • das durch die Schemata beschriebene Format (XML-Struktur, Datentypen etc.) muss eingehalten werden

995 Auf die Durchführung von Positiv- und Negativtestfällen kann verzichtet werden, da die Prüfung auf
996 Schema-Validität bzw. der Umgang mit nicht Schema-validen Nachrichten in den Anwendungsfalltests des
997 WAN erfolgt.

998 3.2.5.4 URI Resource-Tree

999 Der URI Resource-Tree setzt sich aus dem Point-of-Contact (P-o-C) und der im Schema [XSD-COR]
1000 vorgegebenen XML-Struktur zusammen. Die XML-Struktur ist in Abbildung 13 dargestellt.

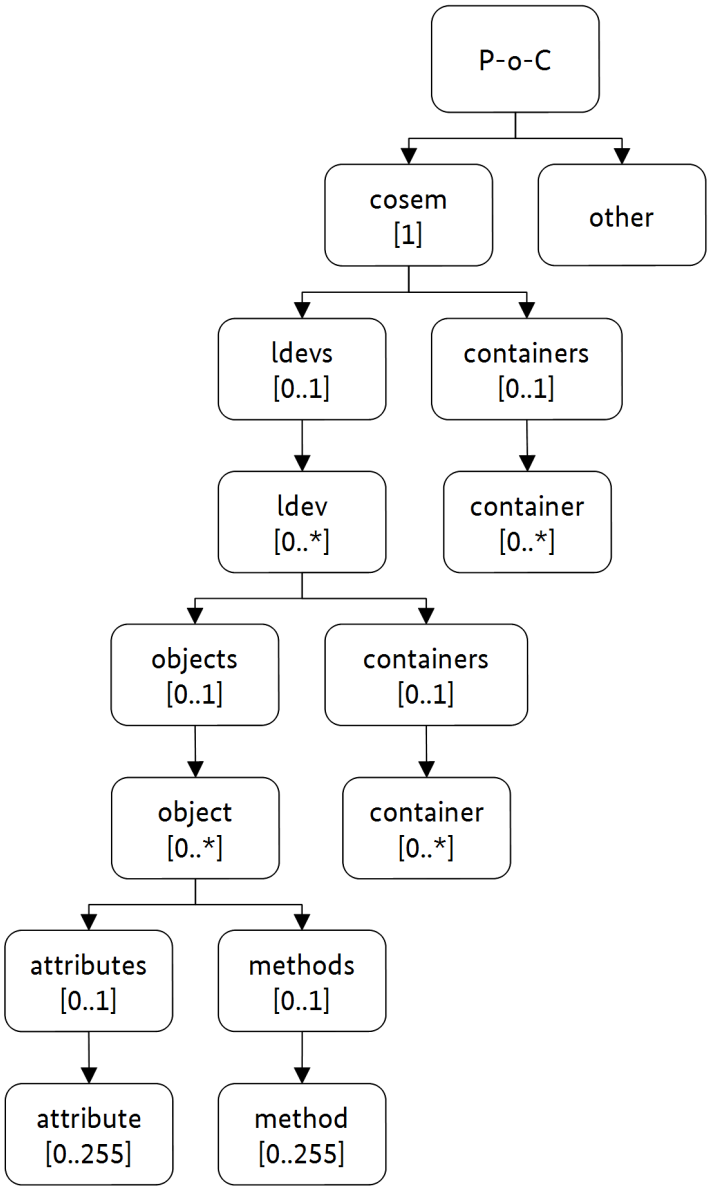

Abbildung 13: XML-Struktur nach XSD-COR

1001 In der folgenden Tabelle sind die XML-Elemente, die zulässigen Operationen auf die Ressourcen und die
1002 Rückgabewerte/Aktionen aufgeführt:

XML-Element	Operation	Rückgabewert / Aktion
cosem	GET	cosem-Element und dessen Unterelemente
ldevs	GET	Liste der Logical Devices und deren Unterelemente
ldev	GET	Liste der Objekte des Logical Devices
	PUT	erzeugt ein neues Logical Device bzw. überschreibt ein bestehendes Logical Device
	DELETE	löscht das Logical Device, das Management Logical Device kann nicht gelöscht werden
containers (cosem)	GET	Liste aller Container
container (cosem)	GET	Inhalt des Containers
	PUT	erzeugt einen neuen Container mit Inhalt bzw. überschreibt den Inhalt eines bestehenden Containers
	DELETE	löscht den Container
objects	GET	Liste aller Objekte des Logical Devices
object	GET	Inhalt des Objekts
	PUT	erzeugt ein neues Objekt mit Inhalt bzw. überschreibt den Inhalt eines bestehenden Objekts
	DELETE	löscht das Objekt
containers (ldev)	GET	Liste aller Container des Logical Devices
container (ldev)	GET	Inhalt des Containers
	PUT	erzeugt einen neuen Container mit Inhalt bzw. überschreibt den Inhalt eines bestehenden Containers
	DELETE	löscht den Container
attributes	GET	Liste aller Attribute des Objekts
attribute	GET	Inhalt des Attributs
	PUT	überschreibt den Inhalt des Attributs
methods	GET	Liste aller Methoden des Objekts
method	POST	ruft die Methode mit den Daten aus dem HTTP-Body des Requests auf

Tabelle 49: XML-Elemente, die zulässigen Operationen und die Rückgabewerte/Aktionen

Um das Verhalten zu prüfen, werden Positiv- und Negativtestfälle durchgeführt.

In den Positivtestfällen sendet der Webservice-Benutzer einen gültigen Request mit der entsprechenden zulässigen Operation an den Webservice-Anbieter. Der Webservice-Anbieter muss den Request verarbeiten und mit einer gültigen Response (HTTP-Status-Code „2xx“ bzw. „5xx“) antworten.

Bei den Negativtestfällen werden vom Webservice-Benutzer ungültige Requests (z. B. unzulässige Operationen) an den Webservice-Anbieter gesendet. Dieser muss die Requests mit einer gültigen Response (HTTP-Status-Code „4xx“) abweisen. Bei den Negativtestfällen werden der Webservice-Benutzer SMGW Administrator und der Webservice-Anbieter SMGW betrachtet, da das SMGW nur gültige Requests erstellen kann und somit die Kombination SMGW → SMGW Administrator ausscheidet.

3.2.5.5 Testeingangskriterien, Abhängigkeiten

Bevor die Tests zur XML Transfersyntax erfolgen können, müssen die Tests für HTTP, TLS und für das SecMod abgeschlossen sein.

3.2.5.6 Testdaten

Für die Tests der XML Transfersyntax müssen im SMGW verschiedene Logische Geräte (Logical Devices wie Zähler, Nutzer etc.) vorhanden sein. Die im HTTP-Body gesendeten Daten müssen den Schemata [XSD-COD] und [XSD-COR] entsprechen und mittels CMS verschlüsselt und signiert sein.

3.2.5.7 Hinweise zu möglichen Testwerkzeugen (informativ)

Für den Test können zum Beispiel folgende Tools eingesetzt werden:

- Smartbear SoapUI
- Parasoft SOAtest

3.2.6 COSEM Interface Classes

Für diesen Abschnitt erwartet das BSI Änderungen an den Bezugsdokumenten. Aus Sicht der Konzeptautoren ist die abstrakte Beschreibung jedoch hinreichend und für den gewählten Testansatz auch erforderlich. Ggf. sind im Rahmen folgender Projektarbeitspakete Anpassungen erforderlich.

Die Modellierung der Datenstrukturen des SMGW muss mit Hilfe der COSEM Interface-Klassen aus dem Standard [IEC 62056-6-1] und den OBIS Codes aus den Standards [IEC 62056-6-2] und [EN 13757-1] geschehen. Um dies zu prüfen, werden Positiv- und Negativtestfälle durchgeführt.

In den Positivtestfällen sendet der Webservice-Benutzer gültige Requests zur Abfrage der Attribute, Methoden, Logical Devices etc. an den Webservice-Anbieter. Der Webservice-Anbieter muss mit einer gültigen Response antworten. Die in der Response zurückgelieferten Klassen-IDs, Attribute und Methoden müssen mit den im Standard [IEC 62056-6-1] definierten Interface Classes übereinstimmen. Weiterhin müssen die Logical-Names der COSEM Objekte/Container korrekt nach den Standards [IEC 62056-6-2] und [EN 13757-1] gebildet wurden sein.

Bei den Negativtestfällen werden vom Webservice-Benutzer ungültige Requests (z. B. falsche Klassen-ID) an den Webservice-Anbieter gesendet. Dieser muss die Requests mit einer gültigen Response (HTTP-Status-Code „4xx“) abweisen. Bei den Negativtestfällen werden der Webservice-Benutzer SMGW Administrator und der Webservice-Anbieter SMGW betrachtet, da das SMGW nur gültige Requests erstellen kann und somit die Kombination SMGW → SMGW Administrator ausscheidet.

3.2.6.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	A	Die geforderte Funktionalität impliziert entsprechende Interoperabilität auf der betrachteten OSI-Schicht.
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	C	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	ja	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	B	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	C	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 50: Bewertungskriterien für WAN / COSEM Interface Classes

3.2.6.2 Testeingangskriterien, Abhängigkeiten

Bevor die Tests zu den COSEM Interface Classes erfolgen können, müssen die Tests für HTTP, TLS und für das SecMod abgeschlossen sein.

3.2.6.3 Testdaten

Für die Tests der COSEM Interface Classes müssen im SMGW verschiedene Logische Geräte (Logical Devices wie Zähler, Nutzer etc.) vorhanden sein. Die im HTTP-Body gesendeten Daten müssen den Schemata [XSD-COD] und [XSD-COR] entsprechen und mittels CMS verschlüsselt und signiert sein.

3.2.6.4 Hinweise zu möglichen Testwerkzeugen (informativ)

Für den Test können zum Beispiel folgende Tools eingesetzt werden:

- Smartbear SoapUI
- Parasoft SOAtest

3.2.7 NTP

Um für das SMGW eine TR-konforme NTP-Implementierung nachzuweisen, muss zum einen getestet werden, inwieweit die gesendeten Pakete der im [RFC5905] geforderten Paketstruktur entsprechen. Zum anderen muss nachgewiesen werden, dass das SMGW die zurückgesendeten NTP-Pakete des SMGW-Admin korrekt behandelt. Dies umfasst sowohl das Abweisen bzw. Nichtverarbeiten von duplizierten, wiederholten oder gefälschten Paketen sowie die korrekte Interpretation der übermittelten Zeitstempel und die daraus resultierende Anpassung der lokalen Systemzeit des SMGW. Weiterhin gilt es zu überprüfen, dass bei Ausfall eines Zeitservers des SMGW-Admin der Schwenk auf einen weiteren Zeitserver reibungslos abläuft.

Da die internen Vorgänge des SMGW im Blackbox-Test nicht untersucht werden können, muss dies mittels Manipulation der Uhrzeit des/der Zeitserver des SMGW-Admin geschehen. Die manipulierte Zeit muss dann im SMGW zu den gewünschten Effekten führen. Dieses Testvorgehen ist näher in Kapitel 4.1.2.2 beschrieben.

Als Protokolltest soll aber die Struktur des NTP-Pakets geprüft werden. Hierfür definiert [BSI TR-03109-1] die zwei Kommunikationsszenarien ntp-over-http (3.2.7.2) und ntp-over-TLS (3.2.7.3).

In diesen Kommunikationsszenarien werden auf die eine oder andere Art und Weise die NTP-Nutzdaten übertragen. Dabei kann überprüft werden, dass das SMGW

- den korrekten Modus verwendet (4 für Client),
- das Stratum einen Wert <2 hat,
- als Reference Clock Identifier die IP des SMGW-Admin eingetragen ist und
- als Reference Timestamp und Originate Timestamp ein gültiges Datum im 64 Bit Zeitstempelformat eingetragen ist.

Der Reference Timestamp muss dabei stets geringer als der Originate Timestamp sein.

3.2.7.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	A	Korrekte Zeitangaben sind insbesondere in Bezug auf Messwertverarbeitung bedeutsam.
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	A	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	ja	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	B	-
	Informativ: bekannte Sicherheitsrisiken und Angriffsszenarien	Auswahl (ja oder nein)	nein	Bekannte Denial-of-Service-Angriffe sind aufgrund der eingesetzten Protokolle nicht praktikabel.
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	A	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 51: Bewertungskriterien für WAN / NTP

3.2.7.2 ntp-over-http

Die in 3.2.7 beschriebenen NTP-Nutzdaten müssen sich in diesem Kommunikationsszenario im HTTP-Body befinden. Weiterhin muss überprüft werden, dass der gesicherte TLS 1.2 Kanal tatsächlich in einem bestimmten Zeitfenster nur Pakete für die Zeitsynchronisation austauscht. Unnötige Informationen im HTTP-Header sollen vermieden werden. In Anlehnung an [BSI TR-03109-1/AII] Tabelle 7 soll ein HTTP-Header der Requests und Responses des SMGW lediglich die dort beschriebenen Muss- und Bedingt-Felder enthalten. Außerdem ist zu überprüfen, dass die ausgetauschten HTTP-Pakete in etwa die gleiche Größe besitzen.

3.2.7.3 ntp-over-TLS

Die in 3.2.7 beschriebenen NTP-Nutzdaten müssen in diesem Kommunikationsszenario direkt über einen gesicherten TLS-1.2-Kanal ausgetauscht werden. Dabei ist sicherzustellen, dass in einem bestimmten Zeitfenster tatsächlich nur Pakete für die Zeitsynchronisation ausgetauscht werden. Vorher ist noch zu überprüfen, dass der TLS-Kanal aufgebaut ist und das erste NTP-Paket erst danach vom SMGW gesendet wird. Der `Originate Timestamp` innerhalb des NTP-Pakets kann hierbei als Quelle für den Zeitpunkt der Erzeugung des NTP-Pakets im SMGW angesehen werden.

3.2.7.4 Testeingangskriterien, Abhängigkeiten

Bevor der Test zu NTP erfolgen kann, müssen die Tests für HTTP, TLS und für das SecMod abgeschlossen sein.

3.2.7.5 Testdaten

Die vom SMGW Administrator gesendeten NTP-Nutzinformationen müssen vollständig dem [RFC5905] entsprechen.

3.2.7.6 Hinweise zu möglichen Testwerkzeugen (informativ)

Für den Test können zum Beispiel folgende Tools eingesetzt werden:

- Smartbear SoapUI
- Parasoft SOAtest
- NTP Time Server Monitor

3.2.8 Wake-Up

Um zu prüfen, dass sich das SMGW bei gültigen und ungültigen Wake-Up Paketen korrekt verhält, werden Positiv- und Negativtestfälle durchgeführt.

Falls das SMGW die Deaktivierung des Wake-Up Services unterstützt, muss zum einen sichergestellt werden, dass der SMGW-Admin den Service deaktivieren kann und zum anderen überprüft werden, dass der Service auch in geeigneter Art wieder aktiviert werden kann.

3.2.8.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	A	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	A	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	ja	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	B	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	A	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 52: Bewertungskriterien für WAN / Wake-Up

3.2.8.2 Tests

Im Positivtestfall werden gültige Wake-Up Pakete nach [BSI TR-03109-1] an den Endpunkt des SMGW versendet, dieses muss daraufhin einen TLS-Kanal zum SMGW Administrator aufbauen.

In den Negativtestfällen werden ungültige Wake-Up Pakete an das SMGW gesendet. Das SMGW darf in diesen Fällen keine Verbindung aufbauen. Ein ungültiges Wake-Up Paket kann z. B. enthalten:

- einen ungültigen Header (z. B. „AB“ statt „WU“)
- eine ungültige Version (z. B. „02h“ statt „01h“)
- einen Zeitstempel (time stamp) weit in der Vergangenheit oder in der Zukunft
- eine falsche Signatur
- einen falschen Adressaten (Geräteidentifikationsdaten des SMGW)

3.2.8.3 Testeingangskriterien, Abhängigkeiten

Bevor die Tests zu Wake-Up erfolgen können, müssen die Tests für das SecMod abgeschlossen sein. Außerdem muss der Erstkonfigurator die Adresse des SMGW-Admin über die lokale Schnittstelle eingebracht haben.

3.2.8.4 Testdaten

Der Endpunkt des SMGW muss bekannt sein und die gültigen Wake-Up Pakete müssen den in [BSI TR-03109-1] beschriebenen Aufbau haben.

3.2.8.5 Hinweise zu möglichen Testwerkzeugen (informativ)

Keine.

3.3 HAN

3.3.1 Ethernet

Die [BSI TR-03109-1] definiert für die HAN-Schnittstelle mindestens das Vorhandensein einer Ethernet-Verbindung mit TCP/IP und empfiehlt die Verwendung von DHCP. Die in [BSI TR-03109-1] vorgegebene Ethernet-Ausprägung ist nicht TR-spezifisch, seit 1990 standardisiert und als bewährte Technologie sowohl im Hinblick auf Implementierungen als auch den Einsatz anzusehen. Eine Detailprüfung dieser Protokollschicht ist daher nicht vorzusehen.[38]

3.3.1.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	C	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	Hier: Ausprägung der Schnittstelle (10/100/1000 MBit)
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	nein	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	ja	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	C	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	A	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 53: Bewertungskriterien für HAN/ Ethernet

38 Hier darf auch davon ausgegangen werden, dass geeignete Testwerkzeuge bei prüfenden Stellen bereits verfügbar sind.

3.3.1.2 Tests

Statische Tests sind als Prüfung der Herstellerdokumentation, hier des Implementation Conformance Statements, vorzusehen.

Ein vollständiger dynamischer Test der Ethernet-Umsetzung an der HAN-Schnittstelle auf Standardkonformität würde den Testumfang deutlich vergrößern, ohne wesentlichen Mehrwert für die Testzielerreichung zu erzeugen und wird deshalb nicht als sinnvoll erachtet. Stattdessen wird durch einzelne dynamische Tests sichergestellt, dass die grundsätzliche Funktionalität der Schnittstelle gegeben ist.

Die Ethernet-Interoperabilität gemäß [IEEE 802.3i] wird geprüft, indem die HAN-Schnittstelle des SMGW mit einer 8P8C-Schnittstelle verbunden und eine Verbindung mit 10 Mbit/s aufgebaut wird. Zusätzlich werden unter Berücksichtigung der aus der Herstellererklärung zur konkreten Schnittstellenimplementierung ermittelten Angaben weitere Verbindungsgeschwindigkeiten (100 Mbit/s, 1000 Mbit/s) geprüft. Wurde mehr als die Mindestanforderung implementiert, entscheidet die Unterstützung weiterer Verbindungsgeschwindigkeiten jedoch nicht über eine erfolgreiche Zertifizierung.

Um dieses Mindestmaß an Interoperabilität bestätigen zu können, sind weiterhin Positivtestfälle zu den Grundtechnologien von Ethernet Bestandteil der Tests.

Dabei werden die folgenden Punkte geprüft:

- Betrieb in den Modi Full- und Half-Duplex,
- Kollisionserkennung und -behandlung nach CSMA/CD,
- Autonegotiation,
- Verschiedene Paketgrößen.

Die Tests prüfen dabei jeweils nur die grundsätzliche Funktionalität und decken nicht alle Besonderheiten und Spezialfälle ab. Es soll ausschließlich die Interoperabilität sichergestellt werden. Aus dem gleichen Grund wird auch geprüft, dass das Address Resolution Protocol im SMGW implementiert ist und damit eine MAC-IP-Zuordnung erfolgen kann. Die genannten Punkte werden geprüft, indem in einzelnen Tests die entsprechende Situationen bzw. Umgebungsparameter simuliert werden und anschließend geprüft wird, dass das SMGW unter diesen Bedingungen kommunizieren kann.

3.3.1.3 Testeingangskriterien, Abhängigkeiten

Hinweis zu den Eingangskriterien: Vom Hersteller muss dokumentiert sein, dass die Ethernetschnittstelle interoperabel zu [IEEE 802.3i] implementiert wurde und ob IPv6 implementiert wurde. Dies ist notwendig, um bestimmen zu können, ob Funktionen auch mit IPv6 getestet werden müssen.

Ansonsten sind bei der Prüfung der Ethernet-Schnittstelle keine Abhängigkeiten zu beachten.

3.3.1.4 Testdaten

Es sind keine weiteren Testdaten zur Prüfung der Ethernet-Schnittstelle notwendig bzw. Nutzdaten für die Tests sind nicht TR-spezifisch zu erstellen.

3.3.1.5 Hinweise zu möglichen Testwerkzeugen (informativ)

Als Testwerkzeug können bestehende Testsuiten wie beispielsweise die des InterOperability Laboratory der Universität New Hampshire genutzt werden.[39]

39 Es können Lizenz- und/oder weitere Kosten anfallen.

3.3.2 Adresszuweisung

[BSI TR-03109-1] erlaubt mehrere Möglichkeiten zur Adresskonfiguration. Diese kann entweder per

- DHCP,
- DHCPv6,
- „Dynamic Configuration of IPv4 Link-Local Addresses“,
- „IPv6 Stateless Address Autoconfiguration“ oder
- manuell

erfolgen. Dabei sollte DHCP und die manuelle Konfiguration unterstützt werden.

3.3.2.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	Hier: Optionale Implementierung (IPv6) beachten
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	nein	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	möglich	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	B	-
	Informativ: bekannte Sicherheitsrisiken und Angriffsszenarien	Auswahl (ja oder nein)	ja	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	A	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 54: Bewertungskriterien für HAN / Adresszuweisung

3.3.2.2 Tests

Zur Prüfung der vier automatischen Varianten soll die Testumgebung die Funktion der Gegenstelle entsprechend des jeweiligen Protokolls bereitstellen. Weiterhin ist zu prüfen, dass das SMGW bei

Verwendung von DHCP nur nach einem DHCPDISCOVER eine neue Adresszuweisung akzeptiert, so dass nicht durch das gezielte Senden eines DHCPOFFER die IP des SMGW manipuliert werden kann.

Um die manuelle Zuweisung der IP-Adresse zu prüfen, wird diese entsprechend der Herstellerdokumentation zugewiesen. Nach einer manuellen Zuweisung sollte sich die IP nicht durch die automatischen Varianten beeinflussen lassen.

3.3.2.3 Testeingangskriterien, Abhängigkeiten

Für den Test der Adresszuweisung muss die Funktionalität der darunterliegenden Ethernet-Schicht gegeben sein.

3.3.2.4 Testdaten

Um die korrekte Zuweisung der IP-Adressen zu prüfen, sind als Testdaten entsprechende Datenpakete zu nutzen. Diese sind Bestandteil der entsprechenden Tests.

3.3.2.5 Hinweise zu möglichen Testwerkzeugen (informativ)

Als Testwerkzeug können bestehende Testsuiten wie beispielsweise die des InterOprerability Laboratory der Universität New Hampshire (https://www.iol.unh.edu) oder ISC Forge (https://bind10.isc.org/wiki/IscForge) genutzt werden. Ebenso kommen hardwareunterstützte Lösungen (z. B. von Agilent Technologies oder Spirent Communications) in Betracht.[40]

3.3.3 TLS

Hinweis: die schnittstellenübergreifenden Testaspekte sind 3.1.2 beschrieben.

3.3.3.1 Testdurchführung

3.3.3.1.1 Dynamische Tests

Folgende schnittstellenspezifischen dynamischen Tests sind vorgesehen:

Anforderungs-referenz	Testfokus	Durchführung	Erwartetes Verhalten
RFC5246.04.04	CertificateRequest	Empfang einer CertificateRequest Nachricht	`certificate_types` und `supported_signature_algorithms` müssen den Anforderungen der TR entsprechen. `certificate_authorities` enthält keine Einträge
RFC5246.04.05	ClientCertificate	Senden einer leeren ClientCertificate Nachricht	Fortsetzen des Handshake

Tabelle 55: Testdurchführung HAN / TLS– Interoperabilität: Verbindung

3.3.4 Identifizierung und Authentifizierung

Hier erwartet der Herausgeber der TR Änderungen mit Version 1.1.

40 Es können Lizenz- und/oder weitere Kosten anfallen.

Die Identifizierung und Authentifizierung von Service-Technikern und CLS gegenüber dem SMGW muss im HAN ausschließlich über HAN-Zertifikate realisiert werden.

3.3.4.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	ja	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	B	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	B	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 56: Bewertungskriterien für HAN / Identifizierung und Authentifizierung

3.3.4.2 Tests

Die Zertifikate müssen den Anforderungen gemäß [BSI TR-03109-1] und [BSI TR-03109-3] entsprechen.

Die Einhaltung dieser Anforderung wird nach einem Verbindungsaufbau durch Positiv- und Negativ-Testfälle geprüft.

Die Anmeldung muss immer erfolgreich sein, wenn das richtige (Identität) und gültige (technische Eigenschaften) Zertifikat verwendet wird. Die Anmeldung darf nicht erfolgreich sein, wenn eine der folgenden Situationen auftritt:

- fehlendes Zertifikat
- gültiges, aber falsches Zertifikat
- richtiges, aber ungültiges Zertifikat
- falsches und ungültiges Zertifikat

Diese Aufstellung stellt einen Überblick der Bereiche dar, in denen Testfälle beschrieben werden müssen. Insbesondere die Tests mit ungültigen Zertifikaten werden aus einer Vielzahl von Testfällen bestehen, die für jede konkrete Anforderung an eine Zertifikatseigenschaft einen Negativtestfall beinhalten.

Für folgende Anwendungsfälle müssen Testfälle entwickelt werden:

- CA-Trust (nur registrierte SM-PKI Zertifikate zulässig)
- Authentifizierung der GWA/EMT/SMGW-Identitäten
- Abgelaufene Zertifikate
- Sperrung von Zertifikaten

Dem Letztverbraucher und Service-Techniker ist es möglich, sich über die HAN-Schnittstelle unter der Angabe des jeweiligen Benutzernamens und des dazugehörigen Passwortes respektive mittels Zertifikat an einer Anzeigeeinheit des SMGW anzumelden. Für die Anmeldung mittels Benutzername/Passwort wird HTTP Digest Access Authentication verwendet.

Benutzerkennungen, die in einem SMGW angelegt werden, müssen eindeutig sein. Es wird also geprüft, ob es möglich ist, mehrere Identitäten mit derselben Benutzerkennung anzulegen. Laut [BSI TR-03109-1] müssen die vergebenen Passworte, welche zu den jeweiligen Benutzerkennungen gehören, den Vorgaben aus [BSI TR-03109-3] entsprechen.

Für den Test der sicheren Implementierung der Benutzername-/Passwort-Authentifizierung wird das Verhalten des SMGW bei Übermittlung falscher Benutzername-Passwort-Kombinationen untersucht. Bei Eingabe einer falschen Kombination muss die Anmeldung fehlschlagen. Ist die Anmeldung fehlgeschlagen, so wird erwartet, dass aus der Fehlermeldung des SMGW nicht darauf geschlossen werden kann, ob der Benutzername und das Passwort fehlerhaft waren, oder nur das Passwort bzw. nur der Benutzername. So kann verhindert werden, dass auf dem System gültige Benutzernamen ermittelt werden.

Der sichere Log-Out-Mechanismus kann im Test verifiziert werden, indem die Reaktion des SMGW auf valide Requests nach dem Log-Out überprüft wird. Erwartungsgemäß werden Requests nur dann ausgeführt, wenn der Benutzer, in dessen Kontext diese ausgeführt werden sollen, am SMGW mit einer gültigen Session angemeldet ist und er berechtigt ist, den entsprechenden Request auszuführen.

3.3.4.3 Testeingangskriterien, Abhängigkeiten

-

3.3.4.4 Testdaten

Sowohl geeignete Zertifikate als auch Anmeldedaten (Benutzerkennungen) für berechtigte Rollen werden benötigt.

3.3.4.5 Testinfrastrukturanforderungen, Hinweise zu möglichen Testwerkzeugen (informativ)

Nachfolgende Tabelle gibt eine Übersicht über die generisch formulierten Anforderungen an eine Testumgebung.

Umgebungsan-forderung	Umzusetzender Standard	Implementierungsmöglichkeiten
(Test-) SM-PKI einschließlich Erzeugung Zertifikate (z. B. für Servicetechniker)	Laut [BSI TR-03109]	-
Zertifikats-überprüfung	Laut [BSI TR-03109-1]	Unter Nutzung OpenSSL oder SSLScan
„HTTP-Tester“, u. a. zur Prüfung der HTTP Digest Authentification	Laut [BSI TR-03109-1]	-

Tabelle 57: Testumgebungsanforderungen HAN / Identifizierung und Authentifizierung

3.3.5 SOCKSv5

Für diesen Abschnitt erwartet das BSI Änderungen an den Bezugsdokumenten. Aus Sicht der Konzeptautoren ist die abstrakte Beschreibung jedoch hinreichend und für den gewählten Testansatz auch erforderlich. Ggf. sind im Rahmen folgender Projektarbeitspakete Anpassungen erforderlich.

Die technische Richtlinie schreibt für HAN die Nutzung von SOCKSv5 zum Aufbau eines transparenten Kanals zu lokalen Systemen vor. Hier wird entsprechend geprüft, ob eine transparente Verbindung zwischen EMT und CLS hergestellt werden kann. Die Verbindung soll dabei von EMT (vermittelt über SMGW-Admin), vom CLS sowie vom SMGW initiiert werden können und darf nur TLS-authentifiziert aufgebaut werden.

3.3.5.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	ja	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	C	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	B	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 58: Bewertungskriterien für HAN / SOCKSv5

3.3.5.2 Testeingangskriterien, Abhängigkeiten

Um zu prüfen, ob die SOCKSv5 Verbindungen korrekt hergestellt werden, muss eine WAN-Verbindung aufgebaut werden können. Weiterhin müssen die in den vorherigen Kapiteln beschriebenen unteren Protokollschichten der HAN-Schnittstelle erfolgreich auf anforderungskonforme Implementierung getestet sein.

3.3.5.3 Testdaten

Zum Aufbau der entsprechenden Verbindungen müssen die entsprechenden Zertifikate erstellt sein und dem SMGW bzw. der Testumgebung zur Verfügung stehen. Zum Testen des transparenten Kanals können dann beliebige Daten übertragen werden.

3.3.5.4 Hinweise zu möglichen Testwerkzeugen (informativ)

Zum Testen der Datenübertragung über den aufgebauten Kanal kann beispielsweise cURL[41] verwendet werden. Für Werkzeuge zum Prüfen der TLS-Zertifikate und -Verbindungen können Hinweise zu Werkzeugen dem Kapitel 3.1.2 entnommen werden.

41 Siehe: http://curl.haxx.se

3.4 LMN

Das SMGW muss an der LMN-Schnittstelle mit drahtlosen und drahtgebundenen Zählern kommunizieren können und daher mindestens zwei Protokollstapel implementieren. Es findet keine Kommunikation zwischen den LMN-Schnittstellen statt, daher können diese unabhängig voneinander getestet werden. Die Testfälle sollen vollständig automatisierbar sein.

3.4.1 Drahtlos

Dieses Kapitel beschreibt die Prüfungen der drahtlosen LMN-Schnittstelle. Es werden nur die in [BSI TR-03109-1] genannten Funkprotokolle im Detail geprüft. Weitere Funkprotokolle sind durch die Tests nicht abgedeckt.

Es ist vorgesehen, so viel wie möglich auf die Spezifikationsergebnisse der OMS-Group zurückzugreifen und diese in die TS aufzunehmen bzw. darauf zu referenzieren[42].

3.4.1.1 Wireless M-Bus

Für die drahtlose Kommunikation ist auf der Ebenen 1 – 3 Wireless M-Bus (wM-Bus) nach [EN 13757-4] vorgeschrieben. Die Feinspezifikation der drahtlosen LMN-Schnittstelle übernimmt hier einige der Vorgaben der Open Metering System Specification Volume 2, Primary Communication, Issue 3.0.1 der OMS Group und erweitert diese mit Vorgaben aus dem OMS-Report [OMS-TR-01].

42 Konkrete Ergebnisse können zum aktuellen Zeitpunkt noch nicht vorweg genommen werden, sondern werden gemeinsam im Projektverlauf zur Erstellung der TS mit dem Herausgeber der TR, der OMS-Group und den Autoren der TS abzustimmen und zu erarbeiten sein.

3.4.1.1.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	A	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	nein	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	möglich	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	B	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	B	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 59: Bewertungskriterien für LMN / Drahtlos / Wireless M-Bus

3.4.1.1.2 Tests

Die aktuelle Version der OMS-Konformitätstests (Version 2.0.0) prüft nur die Konformität von Zählern ab. Im Rahmen der Konformitätsprüfung zur TR sind dabei nur die Tests der drahtlosen Schnittstelle relevant. Diese decken mit den technischen Eigenschaften (PHY) und der Datenübertragung (DLL) die unteren drei Protokollschichten umfassend ab und sollen daher als Hilfestellung bei der Erstellung von Testfällen zur Prüfung der wM-Bus-Konformität des SMGW dienen.

Ein Gerät, welches nach dem Wireless M-Bus-Standard arbeitet, kann verschiedene Funkmodi mit unterschiedlichen Eigenschaften nutzen. Für ein SMGW sind dabei die Modi S1 und T1 für die unidirektionale und S2 und T2 für die bidirektionale Kommunikation relevant. Die OMS Group hat in Version 4 ihrer Open Metering System Specification Volume 2 zusätzlich die Modi C1 und C2 aufgenommen. Diese entsprechen den T-Modi mit veränderter Kodierung. Da diese Modi Bestandteil der nächsten Version der [BSI TR-03109] werden sollen und sich die Tests nicht sehr von denen der anderen Funkmodi unterscheiden, sind auch für diese Testfälle zu erstellen.[43]

Um Kollisionen zu vermeiden darf im Frequenzband 868 – 870 MHz nur in eng begrenzten Zeiträumen gesendet werden. So darf ein Zähler nach [EN 13757-4] nur maximal 0,02 % und das SMGW nur 1% der Zeit senden und damit das Frequenzband nutzen. Dies wird geprüft, indem während der Durchführung der anderen Tests der drahtlosen LMN-Schnittstelle die vom SMGW gesendeten Nachrichten aufgezeichnet und anschließend die Funkbelegung ausgewertet wird. Das SMGW sendet dabei nur in den bidirektionalen Modi S2, T2 und C2.

43 Abhängig zur tatsächlich dann in der nächsten TR-Version veröffentlichten Ausprägung ggf. zu prüfen.

Es wird geprüft, dass das SMGW in den Modi S1/S2 und T1/T2 arbeiten kann. Außerdem wird durch entsprechende Anfragen sichergestellt, dass das SMGW aus den Daten des „Configuration Field“ bzw. des Extended Link-Layers feststellt, ob ein Zähler bidirektionale Kommunikation unterstützt.

Weitere Intervall- und Taktanforderungen beim Empfangen von Zählerwerten und Installations- und Managementdaten werden durch Aufzeichnung der übertragenen Datenpakete während der Prüfung der entsprechenden Funktionen getestet.

Ein Zähler muss die bidirektionale Kommunikation nicht unterstützen oder kann durch die Beschränkungen in der Funkzeit temporär nicht erreichbar sein. Dies wird dem SMGW durch die Link-Control-Bits signalisiert. Hier wird geprüft, dass das SMGW diese Informationen korrekt auswertet und beachtet.

Um Energie zu sparen, stellen mit Batterie betriebene Zähler oft nur direkt nach der Übertragung ein kurzes definiertes Zeitfenster für den Beginn der bidirektionalen Kommunikation zur Verfügung. Hier wird durch Aufzeichnen der vom SMGW gesendeten Daten geprüft, dass die Kommunikation zum richtigen Zeitpunkt beginnt. Ebenso wird geprüft, dass die vom SMGW übertragenen Daten syntaktisch korrekt sind und sich an die Vorgaben der OMS halten, also beispielsweise die Präambel der Nachrichten nur eine bestimmte Länge hat.

Im Data-Link-Layer wird der Nachrichtentyp angegeben und die Kommunikation mittels CRC-Prüfsumme abgesichert. Dabei ist zu prüfen, dass das SMGW nur Nachrichten der Typen

- „SND-NKE“,
- „SND-UD2“,
- „SND-UD“,
- „REQ-UD1“,
- „REQ-UD2“,
- „ACK“ und
- „CNF-IR“

erzeugt.

Weiterhin sind die Typen „SND-NR“ und „RSP-UD“ genau zu prüfen, da über diese beiden Nachrichtentypen Anwendungsdaten, also Messwerte der Zähler, übertragen werden.

Um neue drahtlose Zähler in einem SMGW einzurichten, müssen diese durch den SMGW-Admin angelegt werden und sich außerdem funkseitig mithilfe der Nachrichtentypen „SND-IR“ und „CNF-IR“ beim SMGW melden. Hier wird durch Testfälle dieses funkseitige Registrieren eines neuen Zählers simuliert. Um Probleme mit Zählern zu vermeiden, die fälschlicherweise mehreren Gateways bzw. SMGW zugeordnet sind, soll das SMGW einen Mechanismus implementieren, der solche Probleme auflösen kann. Dies wird geprüft, indem auch dieser Fall simuliert und das Verhalten des SMGW ausgewertet wird.

Das SMGW ist immer der einzige Kommunikationspartner für die Zähler. Daher ist die im Standard vorgesehene Repeaterfunktion für das SMGW ohne Relevanz und muss nicht überprüft werden.

Aufbauend auf der physischen und der Datenübertragungsschicht ist für die drahtlose Übertragung noch ein „Extended Link Layer (ELL)“ vorgesehen. Dieser dient der Fragmentierung von langen Nachrichten. Durch Aufzeichnen und Auswerten der Kommunikation wird sichergestellt, dass der ELL korrekt genutzt und die Werte im Communication Control Field korrekt gesetzt werden. Ebenso wird die standardkonforme Nutzung der CI-Felder und der Adressierung geprüft.

3.4.1.2 OMS Security + AFL

Um die Sicherheit zu erhöhen, ist in [BSI TR-03109-1/AIIIb] ein neuer „Authentication and Fragmentation Layer (AFL)“ definiert. Dieser ist nicht Teil der Open Metering System Specification Volume 2, Primary Communication, Issue 3.0.1 und daher nicht in der Konformitätstestspezifikation der OMS-Group

enthalten. Hier sind dedizierte Testfälle vorzusehen. Außerdem ist zu prüfen, dass mit den anderen in [EN 13757-3] definierten Kryptoverfahren keine Kommunikation möglich ist und daher sichergestellt wird, dass diese durch die TR ausgeschlossenen Verfahren nicht genutzt werden können.

Die Version 4.0.3 der OMS-Spezifikation enthält die in [BSI TR-03109-1/AIIIb] beschriebenen Erweiterungen. Die hierfür geplante Testfälle / Konformitätstests sollen als Grundlage für die Tests des AFL genutzt werden[44].

Der AFL übernimmt drei Aufgaben:

- das Aufteilen langer Nachrichten in kleinere Blöcke,
- eine Nachrichtenauthentifizierung, um die Authentizität für die oberen Schichten zu gewährleisten und
- das Zählen von Nachrichten, wie es für die Schlüsselableitungsfunktion benötigt wird.

3.4.1.2.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	ja	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	C	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	C	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 60: Bewertungskriterien für LMN / Drahtlos / OMS Security + AFL

3.4.1.2.2 Tests

Durch Aufzeichnen und Auswerten der vom SMGW übertragenen Daten wird sichergestellt, dass alle Nachrichten der Typen „SND-UD“, „RSP-UD“, „SND-NR“, „SND-UD“, „RSP-UD“ sowie alle Nachrichten, die TLS-Daten enthalten, den AFL-Layer nutzen und die Felder korrekt gesetzt werden.

Ebenso bzw. durch Senden von Nachrichten mit den entsprechenden (ungültigen) Parametern wird sichergestellt, dass Nachrichten mit ungültiger Kombination aus Verschlüsselung und Authentifizierung vom SMGW weder gesendet noch akzeptiert werden.

44 Ist im Projektverlauf der TS-Erstellung mit der OMS-Group abzustimmen.

3.4.1.3 M-Bus Encryption / Symmetrische Verschlüsselungsverfahren/TLS

Zusätzlich werden für die LMN-Schnittstelle symmetrische kryptographische Verfahren benötigt. Diese werden verwendet, um mit den drahtlos angebundenen Zählern gesichert zu kommunizieren, die nur unidirektional kommunizieren können. Die Anforderungen für die symmetrische Verschlüsselung werden aus der [BSI TR-03109-3] übernommen.

Für die Kommunikation wird zwischen SMGW und Zählern ein gemeinsamer Schlüssel mit 128 Bit nach M-Bus Encryption mit Encryption Mode 7 genutzt. Für die bidirektionale Kommunikation wird stattdessen TLS und damit der Encryption Mode 13 benutzt.

3.4.1.3.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	ja	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	C	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	B	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 61: Bewertungskriterien für LMN / Drahtlos / M-Bus Encryption / Symmetrische Verschlüsselungsverfahren/TLS

3.4.1.3.2 Tests

Um die unidirektionale Kommunikation zu prüfen, wird sowohl mit korrektem, als auch mit ungültigem Schlüssel versucht, Daten nach AES (Encryption Mode 7) an das SMGW zu senden und anschließend die Antwort aufgezeichnet und ausgewertet. Weiterhin wird dasselbe auch mit den Encryption Modes 0 (keine Verschlüsselung) und 5 versucht, um zu prüfen, dass so keine Daten vom SMGW akzeptiert werden.
Auf die gleiche Weise wird der Encryption Mode 13 (TLS) geprüft.

3.4.1.4 M-Bus Application Protokoll

Aufbauend auf der Sitzungsschicht wird das M-Bus Application Protocol nach [EN 13757-3] genutzt. Für das Application Protocol steht durch die Testsuite der OMS-Group bereits eine Möglichkeit zum Prüfen dieser Protokollschicht zur Verfügung. Diese Testsuite soll für die Tests zum M-Bus Application Protocol genutzt werden.

3.4.1.4.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	nein	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	B	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	B	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 62: Bewertungskriterien für LMN / Drahtlos / M-Bus Application Protokoll

3.4.1.4.2 Tests

In den Tests ist sicherzustellen, dass die in [BSI TR-03109-1/AIIIa] festgelegten Daten- und Datensatztypen vom SMGW korrekt unterstützt werden. Die Daten sind dabei den korrekten OBIS-Codes zuzuordnen.

Die Zugriffsnummer identifiziert zusammen mit der Senderaddresse ein Datenpaket. Im Gegensatz zu den Zählern kann das SMGW die Zugriffsnummern für Datenpakete vergleichsweise frei wählen. Es soll dabei nur darauf achten, dass es die gleiche Nummer nicht innerhalb von fünf Minuten für unterschiedliche Datenpakete nutzt. Die korrekte Nutzung der Zugriffsnummer wird, wie der korrekte Aufbau der Datenblöcke, durch Aufzeichnen der übertragenen Daten geprüft. Da die Testumgebung alle Kommunikationspartner des SMGW simuliert und somit die Schlüssel kennt, ist die Verschlüsselung im darunterliegenden AFL-Layer kein Hindernis.

Durch Senden von Nachrichten, in denen über das Statusbyte bestimmte fehlerhafte Zustände an das SMGW gemeldet werden, wird geprüft, dass das SMGW diese Nachrichten korrekt interpretiert und entsprechend auf diese Information reagiert.

Über das Konfigurationsfeld wird unter anderem definiert, welche Verschlüsselung verwendet wird, welche Länge die verschlüsselte Nachricht hat und weitere für die Entschlüsselung wichtige Details. Durch die Tests wird geprüft, dass diese Informationen korrekt vom SMGW gesetzt werden und das SMGW Nachrichten mit fehlerhaften Angaben entsprechend der Vorgabe der TR verarbeitet.

Die Transportschicht mit den beschriebenen Header-Feldern ist bei der drahtlosen Kommunikation vom SMGW zum Zähler immer zu nutzen. Dies ist durch Aufzeichnen und Prüfen der Nachrichten des SMGW sicherzustellen.

Das SMGW muss verschiedene Datentypen und Kodierungen innerhalb des M-Bus-Protokolls unterstützen. Dies wird geprüft, indem Nachrichten mit den entsprechenden Daten an das SMGW gesendet werden und anschließend geprüft wird, dass diese Daten korrekt interpretiert wurden. Dabei ist auch zu prüfen, dass das SMGW bei fehlerhaften Daten die vorgegebene Reaktion ausführt. Außerdem wird getestet, dass das SMGW beim Abrufen von Zählerständen bidirektionaler Zähler die korrekten OBIS-Bezeichner bzw. M-Bus-Tags nutzt.

Weiterhin wird durch Senden entsprechender Datenpakete geprüft, dass das SMGW OBIS-Deklarationen von einem Zähler lernen und anschließend auch diese Daten korrekt auswerten kann.

Das DLMS- und das SML-Anwendungsprotokoll werden von der [BSI TR-03109-1] nicht gefordert und sind daher nicht Bestandteil der Konformitätstests.

3.4.1.4.3 Testeingangskriterien, Abhängigkeiten

Für die meisten der Protokolltests ist es notwendig, dass Zähler im SMGW angelegt wurden. Dies geschieht über die WAN-Schnittstelle, so dass das Anlegen von Zählern und damit auch die Schnittstelle grundsätzlich funktionieren muss. Ansonsten bauen die Protokolltests zu der drahtlosen LMN-Schnittstelle hierarchisch aufeinander auf und haben keine weiteren Abhängigkeiten zu den sonstigen Anwendungsfällen und den Protokolltests der HAN-Schnittstelle. Die LMN-Tests dienen dann als Grundlage für weitere Tests anderer Protokolle und Anwendungsfälle.

3.4.1.4.4 Testdaten

Für die Protokolltests sind keine zusätzlichen Testdaten notwendig.

3.4.1.4.5 Hinweise zu möglichen Testwerkzeugen (informativ)

Da die [BSI TR-03109-1] die Standards zu Wireless M-Bus an einigen Stellen erweitert und eine zusätzliche Sicherungsschicht einführt, können keine Standardwerkzeuge für die Prüfung der drahtlosen LMN-Schnittstelle genutzt werden.

3.4.2 Drahtgebunden

In diesem Kapitel werden die Prüfungen der drahtgebundenen LMN-Schnittstelle beschrieben. Es werden nur die Protokolle geprüft, die in der [BSI TR-03109-1] beschrieben sind. Weitere Anwendungsprotokolle und Datenformate sind nicht Bestandteil der TS.

Es ist vorgesehen, so viel wie möglich auf Arbeitsergebnisse des Forums Netztechnik/Netzbetrieb im VDE und ggf. der DLMS User Organization zurückzugreifen und diese in die TS aufzunehmen bzw. darauf zu referenzieren[45].

45 Konkrete Ergebnisse können zum aktuellen Zeitpunkt noch nicht vorweg genommen werden, sondern werden gemeinsam im Projektverlauf zur Erstellung der TS mit dem Herausgeber der TR, dem FNN und den Autoren der TS abzustimmen und zu erarbeiten sein. Zum aktuellen Stand der FNN-Arbeiten vgl. auch http://www.vde.com/de/fnn/arbeitsgebiete/messwesen/ms2020/Seiten/ms2020dokumente.aspx.

3.4.2.1 EIA/RS-485

Um drahtgebundene Zähler anzubinden, wird EIA/RS-485 genutzt. RS-485 nutzt zur Erhöhung der Toleranz gegen elektromagnetische Störungen eine differentielle Übertragung mit einem Leitungspaar. RS-485 kann durch Variation von Baudrate, Datenformat und den elektrischen Parametern an den konkreten Einsatzzweck angepasst werden. Hier macht der Anhang [BSI TR-03109-1/AIIIa] genaue Vorgaben.

3.4.2.1.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	nein	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	ja	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	C	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	A	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 63: Bewertungskriterien für LMN / Drahtgebunden / EIA/RS-485

3.4.2.1.2 Tests

Durch die [BSI TR-03109-1/AIIIa] ist dabei die Baudrate auf 921,6 kBit/s und das Datenformat auf je ein Start- und Stopp-Bit, 8 Datenbits und kein Paritätsbit festgelegt. Der Abstand zwischen 2 Bits muss dabei kleiner als 2 ms sein. Diese Punkte werden indirekt geprüft, indem bei den Tests der höheren Protokollschichten nur die entsprechenden Parameter genutzt werden. Andere Baudraten oder Datenformate werden nicht geprüft, da sie von der [BSI TR-03109] weder gefordert noch verboten werden.

Der Differenz-Spannungspegel muss beim Empfang mindestens ±200 mV und maximal -7 bis + 12 V betragen. Um dieses Niveau auch mit großen Leitungslängen mit bis über einem Kilometer zu erreichen, muss der Sender auch unter Last mindestens eine Spannung von ±1,5 Volt liefern. Die Spannungen bei einem weniger belasteten Bus müssen außerdem maximal im Bereich -7 bis + 12 liegen. Dies wird getestet, indem die vom SMGW in verschiedenen Lastsituationen an der RS-485-Schnittstelle angelegten Spannungen gemessen werden. Weiterhin wird geprüft, dass das SMGW auch mit entsprechenden Kommunikationspartnern kommunizieren kann, die an der Grenzen der Spannungsbereiche arbeiten.

Der RS-485-Bus ist für bis zu 32 Geräte mit einem Eingangswiderstand von mindestens 12 kΩ ausgelegt. Mit Geräten mit höheren Eingangswiderständen sind auch mehr als 32 Geräte an einem Bus möglich. Es wird geprüft, dass das SMGW auch mit einem Bus korrekt kommuniziert, an dem 31 andere Busteilnehmer aktiv sind. Die anderen Busteilnehmer werden von der Testumgebung simuliert.

Weiterführende Tests sind in der Testsuite vom FNN definiert.

3.4.2.2 HDLC

Zur Sicherung und Vermittlung der Daten zu drahtgebundenen Zählern wird HDLC nach [ISO/IEC 13239] mit FormatType 3 genutzt. Die CRC-Prüfsummen für Header und Frame müssen dabei gemäß der Definition in [IEC 62056-46] erfolgen. Diese Anforderungen werden geprüft, indem die Testumgebung Anfragen mit entsprechenden Nachrichten an das SMGW sendet, die Antworten aufzeichnet und auswertet.

3.4.2.2.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	A	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	A	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	nein	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	möglich	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	C	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	B	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl	ja	-

Tabelle 64: Bewertungskriterien für LMN / Drahtgebunden / HDLC

3.4.2.2.2 Tests

Bei der Verwendung von HDLC sind weitere Timinganforderungen zu beachten, um eine laufende Übertragung zwischen zwei RS-485-Busteilnehmern sicher erkennen zu können und so Störungen zu vermeiden. So darf zwischen zwei Bytes in einem HDLC-Paket nur eine Pause von maximal 10 µs sein. Auf einen HDLC-Request muss innerhalb von einer Millisekunde mit der Antwort begonnen werden. Ein Sender muss maximal 50 µs nach dem Senden wieder abgeschaltet sein und den Bus somit für die nächste Übertragung oder eine Antwort freigegeben haben. Weiterhin darf sich ein Sender frühstens 100 µs nach dem Empfang eines Datenpaketes auf den Bus aufschalten und mit dem Senden einer Antwort beginnen.

Wenn die Antwort nicht innerhalb von einer Millisekunde erfolgt, soll von einem Fehler im Slave ausgegangen werden und der nächste Zähler bzw. derselbe erneut angefragt werden. Wie das erneute Ansprechen erfolgt, also ob der gleiche HDLC-Frame erneut oder ein anderer genutzt wird, wird mittels Parameter im SMWG festgelegt. Ähnlich ist zu verfahren, wenn innerhalb eines Datenpakets die Pausenzeit zwischen einzelnen Zeichen überschritten wird. Die Timinganforderungen werden geprüft, indem die Testumgebung absichtlich entsprechend fehlerhafte Anfragen an das SMGW sendet und die Reaktion auswertet.

Ein weiterer wichtiger Punkt im HDLC-Protokoll ist die Vergabe von Adressen. Anhand der Adressen werden nicht nur die einzelnen Busteilnehmer voneinander unterschieden, sondern auch die Unterscheidung von Protokollen der darüber liegenden Protokollschichten abgebildet. HDLC-Adressen können entweder zwei oder vier Byte lang sein. Dabei dient jeweils das Least-Significant-Byte der Unterscheidung der Protokolle und die sonstigen Bytes dem Adressieren vom LMN-Busteilnehmern. Es können dabei unterschiedliche Adress-Längen für die Datenrichtungen von und zum SMGW genutzt werden.

Die Vergabe von HDLC-Adressen erfolgt nach einem definierten Vorgehen und ist in [BSI TR-03109-1/AIIIa] beschrieben. Das SMGW hat dabei immer die Adresse 0x01 bzw. 0x000001. Die weiteren Busteilnehmer generieren ihre Adresse nach Aufforderung durch das SMGW. Das SMGW hat dabei die Aufgabe, die Eindeutigkeit der generierten Adressen zu gewährleisten und auf Bus-Kollisionen beim Melden der Adressen durch erneutes Senden der bekannten Busteilnehmer zu reagieren. Dies wird geprüft, indem durch die Testumgebung bei der Erkennung neuer Geräte absichtlich Adress- und Bus-Kollisionen erzeugt werden und die Reaktion des SMGW darauf geprüft wird.

Weiterhin muss das SMGW im 30-Sekunden-Takt sowohl nach neuen und als auch nach verstummten Busteilnehmern suchen. Auch hier wird durch Simulation von entsprechendem Verhalten der Busteilnehmer durch die Testumgebung geprüft, dass sich das SMGW wie vorgesehen verhält. Außerdem wird geprüft, dass bereits bekannte Teilnehmer nicht erneut zum Wählen ihrer Adresse aufgefordert werden.

Durch Aufzeichnen und Auswerten der vom SMGW gesendeten Nachrichten wird geprüft, dass das SMGW den Protokollteil der Adresse bei Anfragen an die Zähler korrekt nutzt. Darüber hinaus wird geprüft, dass das SMGW mehrere eingehende Verbindungen mit unterschiedlichen Protokollselektoren unabhängig voneinander verwenden kann und nicht bei einer neuen Anfrage bestehende Verbindungen schließt.

Der Aufbau der einzelnen HDLC-Nachrichten, die das SMGW versendet, sowie die Korrektheit der CRC-Prüfsummen wird mittels der bei anderen HDLC-Protokolltests aufgezeichneten Nachrichten mit geprüft. Weiterhin gehören Tests zum initialen Austausch von Zertifikaten zu den Protokollprüfungen der HDLC-Schicht.

Diese Testfälle orientieren sich an den Tests zur Sicherungsschicht aus den Conformance Tests der DLMS User Association und der Testsuite des FNN. Dabei kann direkt auf Tests des FNN verwiesen werden. Die Tests der DLMS User Association dienen als Hilfe bei der Erstellung weiterer Test für Bereiche, die von Tests des FNN nicht abgedeckt werden und der Überprüfung auf Vollständigkeit der Testabdeckung. Die DLMS User Association betreut die Standards der IEC 62056-Serie und stellt für diese auch Testfälle bereit.

3.4.2.3 TLS

Hinweis: die schnittstellenübergreifenden Testaspekte sind in 3.1.2 beschrieben.

3.4.2.3.1 Testdurchführung

3.4.2.3.1.1 Dynamische Tests

Folgende schnittstellenspezifischen dynamischen Tests sind vorgesehen:

Anforderungs-referenz	Testfokus	Durchführung	Erwartetes Verhalten
RFC5246.04.04	CertificateRequest	Empfang einer CertificateRequest Nachricht	`certificate_types` und `supported_signature_algorithms` müssen den Anforderungen der TR entsprechen. `certificate_authorities` enthält keine Einträge
RFC5246.04.05	ClientCertificate	Senden einer leeren ClientCertificate Nachricht	Abbruch der Verbindung mit `handshake_failure`

Tabelle 65: Testdurchführung LMN / Drahtgebunden / TLS– Interoperabilität: Verbindung

3.4.2.4 SML

Die drahtgebundene Schnittstelle ist aufbauend auf der Absicherung mit TLS als SML nach [IEC 62056-5-3-8] bzw. [BSI TR-03109-1/AIVb] definiert. Die Spezifikation von SML baut stark auf die Verwendung von OBIS-Bezeichnern und COSEM-Objekten nach [IEC 62056-6-1] bzw. [IEC 62056-6-2] auf. Daher wird deren korrekte Nutzung durch die zu erstellenden Tests für SML abgedeckt. Die OBIS-Tests decken sich dabei teilweise mit denen für das WAN-Datenmodell. Durch die gleiche Fachlichkeit soll sich auch die Struktur der Testfälle ähneln. Zur Prüfung von SML werden sowohl Positiv- wie auch Negativtests erstellt. Diese enthalten Tests zur Syntax und der korrekten Verarbeitung der SML-Daten.

1529 3.4.2.4.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	A	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	nein	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	C	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	C	SML-Norm (IEC 62056-5-3-8) soll erst Ende 2014 erscheinen.
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 66: Bewertungskriterien für LMN / Drahtgebunden / SML

1530 3.4.2.4.2 Tests

1531 Die SML-Daten sind nach [BSI TR-03109-1/AIVb] als Datei anzusehen. Es gibt drei Typen von SML-Dateien:

1532 • SML-Auftrags-,

1533 • SML-Antwort- und

1534 • SML-Kombi-Dateien,

1535 die die Nachrichten eines Auftrags und die der dazugehörige(n) Antwort(en) enthalten. Durch die Tests wird
1536 überprüft, dass vom SMGW verschickte Nachrichten sich korrekt an die Beschränkungen der drei
1537 Datentypen halten. Dazu wird geprüft, ob die vom SMGW an das Testsystem versendeten Nachrichten
1538 immer syntaktisch korrekt sind und das SMGW auch fehlerhafte Nachrichten entsprechend der Vorgaben
1539 der [BSI TR-03109-1] verarbeiten kann.

1540 So wird unten anderem durch Aufzeichnen und Auswerten geprüft, dass vom SMGW versendete SML-
1541 Aufträge immer mit genau einer SML_...Open.Req-Nachricht beginnen und immer mit einer einzelnen
1542 SML_...Close.Req-Nachricht enden.

Jede der versendeten Nachrichten ist entweder Anfrage oder Antwort und besteht aus

- einer Transaktions-ID,
- einer Gruppennummer,
- der Angabe wie bei Fehlern verfahren werden soll,
- einer CRC16-Prüfsumme und
- dem Ende der Nachricht.

Die Transaktions-ID wird bei einer Anfrage ein-eindeutig generiert und in den Antwortnachrichten angegeben, um die Zugehörigkeit zum entsprechenden Auftrag zu kennzeichnen. Durch das Senden von Antworten mit den Transaktions-IDs aus den Aufträgen des SMGW wird überprüft, dass die Antworten korrekt zuordnen werden. Weiterhin wird geprüft, dass das SMGW auch Antwortnachrichten ohne Auftrag, also mit einer dem SMGW unbekannten Transaktions-ID korrekt verarbeiten kann.

Über die Gruppennummer kann festgelegt werden, dass bestimmte Nachrichten in einer SML-Datei in einer bestimmten Reihenfolge bzw. parallel zueinander verarbeitet werden können. Die Nachrichten innerhalb einer Gruppe können, müssen aber nicht parallel verarbeitet werden. Dies wird daher nicht geprüft. Weiterhin sind in der [BSI TR-03109-1] keine Aufträge der Zähler an das SMGW vorgesehen, so dass die Gruppen nur von den Zählern und nicht vom SMGW zu beachten und daher nicht zu prüfen sind.

Die CRC16-Checksumme dient der Prüfung der Nachricht. Auf Nachrichten die nicht dekodiert werden können, oder bei denen die Checksumme nicht korrekt ist, soll mit einer „SML-Attention“ geantwortet werden. Dies wird geprüft, indem absichtlich fehlerhafte Nachrichten an das SMGW geschickt werden. Sollte der Fehler bei einer SML_Close-Nachricht auftreten, so ist der Fehler zu ignorieren und eine korrekte SML_CloseRequest-Nachricht muss als Antwort gesendet werden. Sollte die beginnende SML_OpenRequest-Nachricht fehlerhaft sein, so ist die Nachricht zu ignorieren. Auch diese Fälle werden durch entsprechend präparierte Nachrichten geprüft.

SML-Aufträge, die nicht mit einer SML_Open_Request-Nachricht beginnen, sind mit einer SML-Attention-Nachricht mit entsprechendem Error Code zu beantworten und nicht weiter zu verarbeiten. Hier wird durch Senden präparierter SML-Attention-Nachrichten an das SMGW geprüft, dass diese richtig interpretiert werden. Ebenso ist zu testen, dass das SMGW mit Dateien, die nur teilweise gelesen und dekodiert werden können, korrekt umgeht.

Außerdem wird geprüft, dass das SMGW nur Nachrichten versendet, deren Typ in [BSI TR-03109-1/AIVb] definiert ist und auf Aufträge mit unbekannten Typen mit den entsprechenden Fehlern antwortet. Dabei wird auch geprüft, dass das SMGW Aufträge, die nach [BSI TR-03109-1] für Zähler und nicht für das SMGW vorgesehen sind, mit einer Fehlermeldung beantwortet und danach weiterhin korrekt arbeitet.

Die Nachrichtentypen

- SML_GetCosem.Req,
- SML_GetCosem.Res,
- SML_SetCosem.Req,
- SML_SetCosem.Res,
- SML_ActionCosem.Req und
- SML_ActionCosem.Res

werden gesondert und detailliert getestet, da über diese Nachrichtentypen die COSEM-Funktionen „Get“, „Set“ und „Execute“ abgebildet werden. Die Tests der COSEM-Funktionen erfolgen analog zu den in Kapitel 3.2.6 definierten Tests.

Neben der Übertragung von Messdaten als COSEM-Entitäten können Messwerte auch mit weiteren in SML für den Versand von Messwerten vorgesehenen Methoden übertragen werden. So dienen die

Nachrichtentypen SML_GetProfilePack und SML_GetProfileList dem Abrufen von einzelnen Messwerten bzw. von Messwerte-Listen. Zusätzlich kann das SMGW vorparametrisierte Listen mit Datenwerten mit der Anfrage SML_GetList.Req abrufen.

Für alle diese Varianten der Messwerteübertragung wird durch entsprechende, von der Testumgebung an das SMGW gesendete Nachrichten getestet, ob das SMGW diese korrekt empfangen kann. Dabei werden sowohl Messwerte ohne Anfrage an das SMGW gesendet, als auch geprüft, dass das SMGW Aufträge korrekt stellt. So wird sowohl die unidirektionale Kommunikation nach LKS2 als auch die bidirektionale Kommunikation nach LKS1 geprüft.

Durch die Nutzung von präparierten Nachrichten und Auswertung der Antworten wird indirekt geprüft, dass die SML-Daten korrekt kodiert sind bzw. das SMGW die Daten korrekt interpretieren kann.

3.4.3 Zertifikate

Zur gegenseitigen Authentifizierung zwischen SMGW und Zählern im LMN werden X.509 Zertifikate verwendet. Die Zertifikate sind selbst signiert und müssen den strukturellen Anforderungen aus [BSI TR-03109-1] und [BSI TR-03109-3] entsprechen. In den Tests wird geprüft, wie sich das SMGW verhält, wenn gültige und ungültige Zertifikate über die LMN-Schnittstelle angeboten werden, sowie die Struktur der Zertifikate, die das SMGW für LMN-Kommunikationspartner bereitstellt.

3.4.3.1 Testelementbewertung

Bewertungs-ebene	**Kriterium**	**Bewertungs-maßstab**	**Bewertungs-ergebnis**	**Erläuterung / Begründung**
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	nein	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	B	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	B	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 67: Bewertungskriterien für LMN / Zertifikate

3.4.3.2 Tests

Die folgenden Funktionalitäten werden im Test geprüft:

- Generierung von selbst signierten TLS-Zertifikaten
- Einbringung und Erneuerung von TLS-Zertifikaten für bidirektional angeschlossene Meter.

Es wird geprüft, ob die Zertifikate die folgenden Felder und entsprechenden Werte enthalten:

Zertifikatsfeld		Wert
Version	-	V3
SerialNumber	-	Zufällig gewählte, eindeutige Nummer bestimmt vom SMGW (nicht länger als 8 Octets).
Signature	-	Gleicher Wert wie im Feld signatureAlgorithm.
Issuer	-	Leer
Validity	ValidFrom ValidTo	Die Nutzungszeit des Zertifikats ist 7 Jahre.
Subject	-	Leer
SubjectPublicKeyInfo	-	-
Extensions	-	-
SubjectAltName	Othername=<BSI-OID>|| <SMGW/Meter-ID>	Kodierung gemäß Definition der RecipientId laut [BSI TR-03109-3]

Tabelle 68: Zertifikatsfelder

Weiterhin werden Testfälle erstellt, bei denen die Zertifikatsstruktur von den Vorgaben der [BSI TR-03109-1] abweicht. Diese stellen, zusammen mit der Prüfung des Verhaltens beim Versuch abgelaufene Zertifikate zu benutzen, die Negativ-Testfälle dar.

Laut [BSI TR-03109-1] muss das SMGW auch selbst Zertifikate erstellen und an die Zähler übertragen können. Im Test wird geprüft, ob die vom SMGW selbst erstellten LMN-Zertifikate den Vorgaben (Zertifikatsfelder und deren Werte) entsprechen, sowie die Konformität der Übertragung dieser Zertifikate zur [BSI TR-03109-1].

Für den initialen Austausch der vom SMGW bereitgestellten Zertifikate werden symmetrische kryptographische Verfahren, welche in Kapitel 3.4.1.3 - M-Bus Encryption / Symmetrische Verschlüsselungsverfahren/TLS betrachtet werden, genutzt. Nach dem erfolgreichen initialen Übertragen der Zertifikate wird geprüft, ob unmittelbar im Anschluss daran ein TLS-Kanal aufgebaut wird. Über diesen Kanal muss der zählerindividuelle Schlüssel für die Kommunikation mithilfe symmetrischer Kryptographieverfahren gewechselt werden.

Wird das SMGW-Zertifikat aktualisiert, so muss es über den aufgebauten TLS-Kanal an den Zähler gesendet werden können.

3.4.3.3 Testeingangskriterien, Abhängigkeiten

Das Sicherheitsmodul kann selbst erstellte Zertifikate bereitstellen.

Das SMGW kann mittels symmetrischer kryptographischer Verfahren mit den Zählern kommunizieren.

3.4.3.4 Testdaten

- Selbsterstellte Zertifikate
- Zählerindividuelle symmetrische Schlüssel
- Initiale Zählerzertifikate

3.4.3.5 Hinweise zu möglichen Testwerkzeugen (informativ)

Keine.

4 Anwendungsfälle

Kapitel 4 beschreibt die

- schnittstellenspezifischen, funktionalen (Unterkapitel 4.1, 4.2 und 4.3) sowie
- schnittstellenübergreifenden funktionalen Konformitätstests (Unterkapitel 4.4),

die zum Nachweis der anforderungsgemäßen Umsetzung der in [BSI TR-03109-1] definierten Anwendungsfälle durchzuführen sind.

Weiterhin werden Testfälle für nicht-funktionale sonstige Anforderungen definiert (Unterkapitel 4.5).

Um die Erfassung und den Test aller Anwendungsfälle und deren Anforderungen zu gewährleisten, wurde die gesamte [BSI TR-03109-1] vollständig durchlaufen. Die gefundenen Anwendungsfälle und deren Anforderungen wurden anschließend dem jeweiligen Bereich zugeordnet.

Tabelle 69 und Tabelle 70 führen überblicksartig die in [BSI TR-03109-1] definierten Anwendungsfälle auf.

ID	Anwendungsfälle an den Schnittstellen
WAF1	Administration und Konfiguration
WAF2	Zugriff auf Dienste beim SMGW Administrator
WAF3	Alarmierung und Benachrichtigung
WAF4	Übertragung von Daten an den SMGW Administrator
WAF5	Übertragung von Daten an externe Marktteilnehmer
WAF6	Kommunikation EMT mit CLS
WAF7	Wake-Up Service
LAF1	LMN Zählerverwaltung
LAF2	Abruf/Empfang von Messwerten
HAF1	Bereitstellung von Daten für den Letztverbraucher
HAF2	Bereitstellung von Daten für den Service-Techniker
HAF3	Transparenter Kommunikationskanal zwischen CLS und EMT

Tabelle 69: Anwendungsfälle an den SMGW-Schnittstellen

ID	Schnittstellenübergreifende Anwendungsfälle
TAF1	Datensparsame Tarife
TAF2	Zeitvariable Tarife
TAF3	Lastvariable Tarife
TAF4	Verbrauchsvariable Tarife
TAF5	Ereignisvariable Tarife
TAF6	Abruf von Messwerten im Bedarfsfall
TAF7	Zählerstandsgangmessung
TAF8	Erfassung von Extremwerten für Leistung
TAF9	Abruf der Ist-Einspeisung einer Erzeugungsanlage
TAF10	Abruf von Netzzustandsdaten

Tabelle 70: Anwendungsfälle schnittstellenübergreifend

4.1 WAN

Innerhalb der [BSI TR-03109-1] werden verschiedene Anwendungsfälle formuliert, die nicht durch Einzeltests im Rahmen der Interoperabilität abgeprüft werden können. Um nachzuweisen, dass die Anwendungsfälle mit dem zu testenden Smart Meter Gateway abgearbeitet werden können, werden in der Testspezifikation Testfälle und Testfallketten definiert, mit dem die Anwendungsfälle nachgestellt werden.[46]

Die Anwendungsfälle an der WAN Schnittstelle können in folgende Kategorien eingeteilt werden:

- Administration und Konfiguration des Smart Meter Gateways durch den SMGW Administrator
- Zugriff des SMGW auf Dienste beim SMGW Administrator
- Alarmierung und Benachrichtigung des SMGW Administrators bei Auftreten von (unerwarteten) Ereignissen im SMGW
- Übertragung von Daten an den SMGW Administrator. Die übertragenen Daten können entweder für den SMGW Administrator bestimmt sein oder auch für einen Dritten. Dies ist z. B. bei der pseudonymisierten Übertragung von Netzzustandsdaten der Fall.
- Übertragung von Daten an externe Marktteilnehmer
- Kommunikation externer Marktteilnehmer mit einem CLS über das SMGW
- Wake-Up Service

Die sieben Anwendungsfälle nutzen die folgenden fünf Kommunikationsszenarien, die vom SMGW unterstützt werden MÜSSEN:

- WKS1: MANAGEMENT (Administration)
- WKS2: ADMIN-SERVICE
- WKS3: INFO-REPORT
- WKS4: NTP-HTTPS
- WKS5: NTP-TLS

46 Eine Reihe von Punkten der WAN-Spezifikation befindet sich in Klärung beim Herausgeber der TR (z. B. Ablauf beim Löschen/Deaktivieren von Geräten (in WAF1)) bzw. es werden noch Änderungen an der Bezugsdokumentation vorgenommen (z. B. COD/COR, Firmwareupload/-download). An diesen Stellen können sich im weiteren Verlauf der Testspezifikationserstellung noch Änderungen ergeben.

4.1.1 WAF1: Administration und Konfiguration

Der WAF1 umfasst sehr viele Anforderungen. Aus diesem Grund wird dieser Anwendungsfall in verschiedene Szenarien eingeteilt. Durch die Negativtestfälle werden auch die beiden Anforderungen „Administration nur durch den SMGW Administrator“ und „keine Administration durch Dritte“ getestet und abgedeckt. Alle Szenarien nutzen das Kommunikationsszenario „MANAGEMENT“.

Der Ablauf aller Positivtestfälle gestaltet sich wie folgt:

- Der Webservice-Benutzer SMGW Administrator sendet einen gültigen Request an den Webservice-Anbieter SMGW.
- In Abhängigkeit vom verwendeten Dienst werden ggf. relevante Daten als XML-Struktur an das SMGW übergeben.
- Das SMGW muss den gültigen Request verarbeiten und mit einer gültigen Response antworten.
- Ob die Ressource angelegt, geändert oder gelöscht wurde, wird mit Hilfe des Get-Dienstes geprüft.

In den Positivtestfällen werden u. a. folgende Punkte geprüft:

- korrektes Verhalten bei unterschiedlich befüllter XML-Struktur (z. B. nur Befüllung der Pflichtfelder der XML-Struktur, Befüllung aller Felder der XML-Struktur)
- korrektes Verhalten bei der Verarbeitung von Grenzwerten

Der Ablauf aller Negativtestfälle gestaltet sich wie folgt:

- Der Webservice-Benutzer SMGW Administrator sendet einen gültigen bzw. ungültigen Request an den Webservice-Anbieter SMGW.
- In Abhängigkeit vom verwendeten Dienst werden ggf. relevante Daten als XML-Struktur an das SMGW übergeben.
- Das SMGW muss den gültigen bzw. ungültigen Request verarbeiten und mit einer gültigen Response antworten.
- Ob die Ressource nicht angelegt, geändert oder gelöscht wurde, wird mit Hilfe des Get-Dienstes geprüft.

In den Negativtestfällen werden u. a. folgende Punkte geprüft:

- Verhalten bei Schema-invaliden Requests (z. B. falsche XML-Struktur und Werte außerhalb des definierten Wertebereichs [Grenzwerte])
- Abweisen von Requests mit falscher XML Inhaltskodierung

Ist in einem Request eine XML-Struktur vorhanden, so muss diese auf Schema-Validität (siehe XSD Schema Relation) und korrekte Inhaltskodierung (siehe XML Inhaltskodierung) geprüft werden. Weiterhin muss geprüft werden, dass die im Request enthaltenen dienstabhängigen Daten CMS verschlüsselt vorliegen. Die jeweilige Prüfung kann bei den Negativtestfällen entfallen, die das Verhalten bei Schema-Invalidität bzw. falscher Inhaltskodierung testen.

Besonderheiten der verschiedenen Szenarien bzw. Abweichungen von dem oben beschriebenen Vorgehen werden in den entsprechenden Kapiteln beschrieben.

Werden in einem Positivtestfall in einem Szenario Daten in das SMGW eingebracht und wird dieser Positivtestfall bestanden, dann können diese eingebrachten Daten für darauffolgende Positivtestfälle in diesem Szenario genutzt werden. Sind alle Positivtestfälle eines Szenarios bestanden und die eingebrachten Daten sind nach einer erneuten Prüfung noch immer valide, dann können diese auch für Negativtestfälle in diesem Szenario verwendet werden. Sind die eingebrachten Daten nicht mehr valide, dann können neue valide Daten über den entsprechenden Positivtestfall eingebracht, geprüft und für den Negativtestfall verwendet werden. Soweit möglich sollen Testfälle stets auch einzeln ausgeführt werden können.

4.1.1.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	C	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	A	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	ja	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	A	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	A	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 71: Bewertungskriterien für WAF1: Administration und Konfiguration

4.1.1.2 Geräteverwaltung

Das SMGW muss nach [BSI TR-03109-1] dem SMGW Administrator folgende Funktionalität zur Verfügung stellen:

- der SMGW Administrator muss Geräte (z. B. Zähler, CLS und Anzeigeeinheiten) im SMGW registrieren können
- der SMGW Administrator muss Geräte einem Letztverbraucher zuordnen können

Um diese Funktionalität zu testen, werden Positiv- und Negativtestfälle erstellt.

In den Positivtestfällen werden folgende Dienste genutzt und decken die Funktionalitäten entsprechend ab:

Dienst	Funktionalität
Create	Zähler registrieren CLS registrieren Anzeigeeinheit registrieren
Set	Zähler einem Letztverbraucher zuordnen CLS einem Letztverbraucher zuordnen Anzeigeeinheit einem Letztverbraucher zuordnen

Tabelle 72: Dienste und Funktionalitäten

Bei den Negativtestfällen werden zusätzlich folgende Fehlerszenarien geprüft:

- keine Geräteanlage durch einen unberechtigten Webservice-Benutzer (EMT, Letztverbraucher, Servicetechniker)
- keine Geräteanlage, wenn ein falsches Geräteprofil übergeben wird (wird ggf. durch den Test des Verhaltens bei Schema-invaliden Requests abgedeckt)
- keine Gerätezuordnung zu einem Letztverbraucher durch einen unberechtigten Webservice-Benutzer (EMT, Letztverbraucher, Servicetechniker)

Mit Hilfe des Get-Dienstes wird bei den Negativtestfällen geprüft, dass die in der Request-URI angegebene Ressource nicht angelegt bzw. geändert wurde.

4.1.1.2.1 Testeingangskriterien, Abhängigkeiten

Bevor die Tests zur Geräteverwaltung im WAF1 erfolgen können, müssen alle Protokolltests, der Test der Mandantenverwaltung und der Test des SecMod erfolgreich abgeschlossen worden sein. Der SMGW Administrator muss sich mit dem SMGW verbinden können und muss mit einem gültigen Zertifikat und Kommunikationsadresse im SMGW eingerichtet sein. Mehrere Letztverbraucher müssen im SMGW administriert sein (es können z. B. die in der Mandatenverwaltung angelegten Letztverbraucher genutzt werden). Die Testdaten müssen verfügbar sein.

4.1.1.2.2 Testdaten

Für die Tests der Geräteverwaltung müssen folgende Testdaten vorhanden sein:

-
- es müssen verschiedene Daten für mehrere Zähler, CLS und Anzeigeeinheiten für die Befüllung der XML-Struktur vorhanden sein

Eine konkrete Aussage über die Menge an benötigten Daten für die Zähler, CLS und Anzeigeeinheiten kann aktuell nicht getroffen werden, da die Schemata [XSD-COD] und [XSD-COR] nicht final vorliegen und der Aufbau der XML-Struktur somit noch nicht konkret feststeht und z. B. eine Äquivalenzklassenbildung damit nicht möglich ist.

4.1.1.2.3 Hinweise zu möglichen Testwerkzeugen (informativ)

Für den Test können zum Beispiel folgende Tools eingesetzt werden:

- Smartbear SoapUI
- Parasoft SOAtest

4.1.1.3 Mandatenverwaltung

Das SMGW muss nach [BSI TR-03109-1] dem SMGW Administrator folgende Funktionalität zur Verfügung stellen:

- Anlage, Bearbeitung und Löschung von Letztverbrauchern
- Anlage, Zuordnung und Löschung von Zertifikaten bzw. Userid/Passwort zu einem Letztverbraucher

Um diese Funktionalität zu testen, werden Positiv- und Negativtestfälle erstellt.

In den Positivtestfällen werden folgende Dienste genutzt und decken die Funktionalitäten entsprechend ab:

Dienst	Funktionalität
Create	Letztverbraucher anlegen Userid/Passwort anlegen Zertifikat anlegen
Set	Letztverbraucher bearbeiten Userid/Passwort zuordnen Zertifikat zuordnen
Delete	Letztverbraucher löschen Userid/Passwort löschen Zertifikat löschen

Tabelle 73: Dienste und Funktionalitäten

Bei den Negativtestfällen werden zusätzlich folgende Fehlerszenarien geprüft:

- keine Anlage, Bearbeitung und Löschung von Letztverbrauchern durch einen unberechtigten Webservice-Benutzer (EMT, Letztverbraucher, Servicetechniker)
- keine Anlage, Zuordnung und Löschung von Zertifikaten bzw. Userid/Passwort zu einem Letztverbraucher durch einen unberechtigten Webservice-Benutzer (EMT, Letztverbraucher, Servicetechniker)
- keine Anlage von Letztverbrauchern, Zertifikaten und Userid/Passwort, wenn falsche Daten übergeben werden (wird ggf. durch den Test des Verhaltens bei Schema-invaliden Requests abgedeckt)

Mit Hilfe des Get-Dienstes wird bei den Negativtestfällen geprüft, dass die in der Request-URI angegebene Ressource nicht angelegt, geändert, zugeordnet bzw. gelöscht wurde.

4.1.1.3.1 Testeingangskriterien, Abhängigkeiten

Bevor die Tests zur Mandantenverwaltung im WAF1 erfolgen können, müssen alle Protokolltests und der Test des SecMods erfolgreich abgeschlossen worden sein. Der SMGW Administrator muss sich mit dem SMGW verbinden können und er muss mit einem gültigen Zertifikat und seiner Kommunikationsadresse im SMGW eingerichtet sein. Die Testdaten müssen verfügbar sein.

4.1.1.3.2 Testdaten

Für die Tests der Mandantenverwaltung müssen folgende Testdaten vorhanden sein:

- Es müssen verschiedene Daten für mehrere Letztverbraucher für die Befüllung der XML-Struktur vorhanden sein.

Eine konkrete Aussage über die Menge an benötigten Daten für die Letztverbraucher kann aktuell nicht getroffen werden, da die Schemata [XSD-COD] und [XSD-COR] nicht final vorliegen und der Aufbau der XML-Struktur somit noch nicht konkret feststeht und z. B. eine Äquivalenzklassenbildung damit nicht möglich ist.

4.1.1.3.3 Hinweise zu möglichen Testwerkzeugen (informativ)

Für den Test können zum Beispiel folgende Tools eingesetzt werden:

- Smartbear SoapUI
- Parasoft SOAtest

4.1.1.4 Profilverwaltung

Das SMGW muss nach [BSI TR-03109-1] dem SMGW Administrator folgende Funktionalität zur Verfügung stellen:

- Anlage, Aktivierung und Löschung von Zähler-, Kommunikations- und Auswertungsprofilen

Um diese Funktionalität zu testen, werden Positiv- und Negativtestfälle erstellt.

In den Positivtestfällen werden folgende Dienste genutzt und decken die Funktionalitäten entsprechend ab:

Dienst	Funktionalität
Create	Zählerprofil anlegen Kommunikationsprofil anlegen Auswertungsprofil anlegen
Set	Zählerprofil aktivieren Kommunikationsprofil aktivieren Auswertungsprofil aktivieren
Delete	Zählerprofil löschen Kommunikationsprofil löschen Auswertungsprofil löschen

Tabelle 74: Dienste und Funktionalitäten

Bei den Negativtestfällen werden zusätzlich folgende Fehlerszenarien geprüft:

- keine Anlage, Aktivierung und Löschung von Zähler-, Kommunikations- und Auswertungsprofilen durch einen unberechtigten Webservice-Benutzer (EMT, Letztverbraucher, Servicetechniker)
- keine Anlage, Aktivierung und Löschung von Zähler-, Kommunikations- und Auswertungsprofilen, wenn falsche Daten übergeben werden (wird ggf. durch den Test des Verhaltens bei Schema-invaliden Requests abgedeckt)

Mit Hilfe des Get-Dienstes wird bei den Negativtestfällen geprüft, dass die in der Request-URI angegebene Ressource nicht angelegt, geändert, zugeordnet bzw. gelöscht wurde.

4.1.1.4.1 Testeingangskriterien, Abhängigkeiten

Bevor die Tests zur Profilverwaltung im WAF1 erfolgen können, müssen alle Protokolltests und der Test des SecMods erfolgreich abgeschlossen worden sein. Der SMGW Administrator muss sich mit dem SMGW verbinden können und er muss mit einem gültigen Zertifikat und seiner Kommunikationsadresse im SMGW eingerichtet sein. Die Testdaten müssen verfügbar sein.

4.1.1.4.2 Testdaten

Für die Tests der Profilverwaltung müssen folgende Testdaten vorhanden sein:

- Es müssen verschiedene Daten für mehrere Zähler-, Kommunikations- und Auswertungsprofile für die Befüllung der XML-Struktur vorhanden sein.

Eine konkrete Aussage über die Menge an benötigten Daten für die Zähler-, Kommunikations- und Auswertungsprofile kann aktuell nicht getroffen werden, da die Schemata [XSD-COD] und [XSD-COR] nicht final vorliegen und der Aufbau der XML-Struktur somit noch nicht konkret feststeht und z. B. eine Äquivalenzklassenbildung damit nicht möglich ist.

4.1.1.4.3 Hinweise zu möglichen Testwerkzeugen (informativ)

Für den Test können zum Beispiel folgende Tools eingesetzt werden:

- Smartbear SoapUI
- Parasoft SOAtest

4.1.1.5 Schlüssel-/Zertifikatsmanagement

Das SMGW muss nach [BSI TR-03109-1] dem SMGW Administrator folgende Funktionalität zur Verfügung stellen:

- Anlage, Aktivierung, Deaktivierung und Löschung von Zertifikaten und Schlüsseln für die Kommunikation der Zähler, CLS und EMT mit dem SMGW

In den Positivtestfällen werden folgende Dienste genutzt und decken die Funktionalitäten entsprechend ab:

Dienst	Funktionalität
Create	Zertifikat anlegen Schlüssel anlegen
Set	Zertifikat aktivieren/deaktivieren Schlüssel aktivieren/deaktivieren
Delete	Zertifikat löschen Schlüssel löschen

Tabelle 75: Dienste und Funktionalitäten

Bei den Negativtestfällen werden zusätzlich folgende Fehlerszenarien geprüft:

- keine Anlage, Aktivierung, Deaktivierung und Löschung von Zertifikaten und Schlüsseln für die Kommunikation der Zähler, CLS und EMT mit dem SMGW durch einen unberechtigten Webservice-Benutzer (EMT, Letztverbraucher, Servicetechniker)
- keine Anlage, Aktivierung, Deaktivierung und Löschung von Zertifikaten und Schlüsseln für die Kommunikation der Zähler, CLS und EMT mit dem SMGW, wenn falsche Daten übergeben werden (wird ggf. durch den Test des Verhaltens bei Schema-invaliden Requests abgedeckt)

Mit Hilfe des Get-Dienstes wird bei den Negativtestfällen geprüft, dass die in der Request-URI angegebene Ressource nicht angelegt, geändert, zugeordnet bzw. gelöscht wurde.

4.1.1.5.1 Testeingangskriterien, Abhängigkeiten

Bevor die Tests zum Schlüssel- und Zertifikatsmanagement im WAF1 erfolgen können, müssen alle Protokolltests und der Test des SecMods erfolgreich abgeschlossen worden sein. Der SMGW Administrator muss sich mit dem SMGW verbinden können und er muss mit einem gültigen Zertifikat und seiner Kommunikationsadresse im SMGW eingerichtet sein. Die Testdaten müssen verfügbar sein.

4.1.1.5.2 Testdaten

Für die Tests des Schlüssel-/Zertifikatsmanagement müssen folgende Testdaten vorhanden sein:

- Es müssen verschiedene Daten für mehrere Zertifikate und Schlüssel für die Befüllung der XML-Struktur vorhanden sein.

Eine konkrete Aussage über die Menge an benötigten Daten für die Zertifikate und Schlüssel kann aktuell nicht getroffen werden, da die Schemata [XSD-COD] und [XSD-COR] nicht final vorliegen und der Aufbau

der XML-Struktur somit noch nicht konkret feststeht und z. B. eine Äquivalenzklassenbildung damit nicht möglich ist.

4.1.1.5.3 Hinweise zu möglichen Testwerkzeugen (informativ)

Für den Test können zum Beispiel folgende Tools eingesetzt werden:

- Smartbear SoapUI
- Parasoft SOAtest

4.1.1.6 Firmware-Update

Das SMGW muss es dem SMGW Administrator erlauben, neue Firmware in das SMGW aufzuspielen, zu verifizieren und zu aktivieren. Um diese Funktionalität zu testen, werden Positiv- und Negativtestfälle erstellt.

In den Positivtestfällen sendet der Webservice-Benutzer SMGW Administrator gültige Requests an den Webservice-Anbieter SMGW. Im HTTP-Body werden ggf. die relevanten Daten für das Firmware-Update an das SMGW übergeben. Das SMGW muss den gültigen Request verarbeiten. Das SMGW antwortet anschließend mit einer gültigen Response und dem HTTP-Status-Code „200“. Folgende Dienste werden genutzt und decken die Funktionalitäten entsprechend ab:

Dienst	Funktionalität
Notify (Event)	Firmware-Update und -Download auslösen

Tabelle 76: Dienste und Funktionalitäten

Bei den Negativtestfällen werden gültige Requests von nicht berechtigten Webservice-Benutzern (EMT, Letztverbraucher, Servicetechniker) zum Firmware-Update an den Webservice-Anbieter SMGW gesendet. Das SMGW muss diese Requests wegen fehlender Berechtigung mit einem HTTP-Status-Code „4xx“ abweisen. Weiterhin wird eine fehlerhafte Firmware zum Download zur Verfügung gestellt. Diese fehlerhafte Firmware darf sich nicht in das SMGW einspielen lassen.

4.1.1.6.1 Testeingangskriterien, Abhängigkeiten

Bevor die Tests zum Firmware-Update im WAF1 erfolgen können, müssen alle Protokolltests und der Test des SecMods erfolgreich abgeschlossen worden sein.

4.1.1.6.2 Testdaten

Die im HTTP-Body gesendeten Daten müssen den Schemata [XSD-COD] und [XSD-COR] entsprechen und mittels CMS verschlüsselt und signiert sein.

4.1.1.6.3 Hinweise zu möglichen Testwerkzeugen (informativ)

Für den Test können zum Beispiel folgende Tools eingesetzt werden:

- Smartbear SoapUI
- Parasoft SOAtest

4.1.1.7 Wake-Up Konfiguration

Das SMGW muss nach [BSI TR-03109-1] dem SMGW Administrator folgende Funktionalität zur Verfügung stellen:

- Konfiguration der Adresse des Wake-Up Service

Um diese Funktionalität zu testen, werden Positiv- und Negativtestfälle erstellt.

In den Positivtestfällen wird folgender Dienst genutzt und deckt die Funktionalitäten entsprechend ab:

Dienst	Funktionalität
Set	Adresse des Wake-Up Service bearbeiten

Tabelle 77: Dienst und Funktionalität

Bei den Negativtestfällen werden zusätzlich folgende Fehlerszenarien geprüft:

- keine Konfiguration der Adresse des Wake-Up Service durch einen unberechtigten Webservice-Benutzer (EMT, Letztverbraucher, Servicetechniker)
- keine Konfiguration der Adresse des Wake-Up Service, wenn falsche Daten übergeben werden (wird ggf. durch den Test des Verhaltens bei Schema-invaliden Requests abgedeckt)

Mit Hilfe des Get-Dienstes wird bei den Negativtestfällen geprüft, dass die in der Request-URI angegebene Ressource nicht angelegt, geändert, zugeordnet bzw. gelöscht wurde.

4.1.1.7.1 Testeingangskriterien, Abhängigkeiten

Bevor die Tests zur Wake-Up Konfiguration im WAF1 erfolgen können, müssen alle Protokolltests und der Test des SecMods erfolgreich abgeschlossen worden sein. Der SMGW Administrator muss sich mit dem SMGW verbinden können und er muss mit einem gültigen Zertifikat und seiner Kommunikationsadresse im SMGW eingerichtet sein. Weiterhin muss eine gültige Adresse für den Wake-Up Service im SMGW eingerichtet sein. Die Testdaten müssen verfügbar sein.

4.1.1.7.2 Testdaten

Für die Tests der Wake-Up Konfiguration müssen folgende Testdaten vorhanden sein:

- Es müssen mehrere verschiedene Adressen des Wake-Up Service für die Befüllung der XML-Struktur vorhanden sein.

Eine konkrete Aussage über die Menge an benötigten Daten für die Wake-Up Konfiguration kann aktuell nicht getroffen werden, da die Schemata [XSD-COD] und [XSD-COR] nicht final vorliegen und der Aufbau der XML-Struktur somit noch nicht konkret feststeht und z. B. eine Äquivalenzklassenbildung damit nicht möglich ist.

4.1.1.7.3 Hinweise zu möglichen Testwerkzeugen (informativ)

Für den Test können zum Beispiel folgende Tools eingesetzt werden:

- Smartbear SoapUI
- Parasoft SOAtest

4.1.1.8 SMGW Monitoring

Das SMGW muss nach [BSI TR-03109-1] dem SMGW Administrator folgende Funktionalität zur Verfügung stellen:

- Zustands des SMGW abfragen
- Logeinträge aus dem System- und eichtechnischen Log auslesen

Um diese Funktionalität zu testen, werden Positiv- und Negativtestfälle erstellt.

1904 In den Positivtestfällen wird folgender Dienst genutzt und deckt die Funktionalitäten entsprechend ab:

Dienst	Funktionalität
Get	Zustand abfragen Systemlog auslesen eichtechnisches Log auslesen

Tabelle 78: Dienste und Funktionalitäten

1905 Weiterhin wird in den Positivtestfällen getestet, dass die ausgelesenen Daten in einer XML-Struktur
1906 schemakonform bereitgestellt werden und folgende Informationen enthalten:

1907 • record_number
1908 • datetime
1909 • level
1910 • event_type
1911 • subject_identity
1912 • outcome
1913 • message
1914 • user_identity
1915 • destination
1916 • evidence

1917 Bei den Negativtestfällen werden zusätzlich folgende Fehlerszenarien geprüft:

1918 • keine Abfrage des Zustands des SMGW und der Logs durch einen unberechtigten Webservice-Benutzer
1919 (EMT, Letztverbraucher, Servicetechniker)

1920 4.1.1.8.1 Testeingangskriterien, Abhängigkeiten

1921 Bevor die Tests zum SMGW Monitoring im WAF1 erfolgen können, müssen alle Protokolltests und der Test
1922 des SecMods erfolgreich abgeschlossen worden sein. Der SMGW Administrator muss sich mit dem SMGW
1923 verbinden können und er muss mit einem gültigen Zertifikat und seiner Kommunikationsadresse im
1924 SMGW eingerichtet sein. Das SMGW muss sich in einem auslesbaren Zustand befinden und die Testdaten
1925 müssen verfügbar sein.

1926 4.1.1.8.2 Testdaten

1927 Für die Tests des SMGW Monitoring müssen folgende Testdaten vorhanden sein:

1928 • Im System- und eichtechnischen Log müssen sich jeweils mehrere Ereignisse befinden.

1929 Die im System- und eichtechnischen Log hinterlegten Ereignisse könnten zum Beispiel durch die
1930 Testumgebung „provoziert“ werden. Möglichkeiten wären zum Beispiel:

1931 • Ausfall der WAN-Verbindung
1932 • keine Möglichkeit zur Zeitsynchronisation
1933 • technische falsche Messwerte werden vom Zähler an das SMGW gesendet.

1934 4.1.1.8.3 Hinweise zu möglichen Testwerkzeugen (informativ)

1935 Für den Test können zum Beispiel folgende Tools eingesetzt werden:

- Smartbear SoapUI
- Parasoft SOAtest

4.1.2 WAF2: Zugriff auf Dienste beim SMGW Administrator

Der WAF2 umfasst viele Anforderungen. Aus diesem Grund wird dieser Anwendungsfall in verschiedene Szenarien eingeteilt. Sind alle Szenarien bestanden, gilt auch die Anforderung „Dienste, auf die das SMGW im Betrieb angewiesen ist, muss das SMGW beim SMGW Administrator aufrufen können“ als bestanden. Alle Szenarien nutzen das Kommunikationsszenario „ADMIN-SERVICE“.

Der Ablauf aller Positivtestfälle gestaltet sich wie folgt:

- Der Webservice-Benutzer SMGW sendet einen gültigen Request an den Webservice-Anbieter SMGW Administrator.
- In Abhängigkeit vom verwendeten Dienst werden ggf. relevante Daten als XML-Struktur an das SMGW übergeben.
- Der SMGW Administrator sendet eine gültige Response.
- Das SMGW muss die vom SMGW Administrator gesendete gültige Response verarbeiten.

In den Positivtestfällen werden u. a. folgende Punkte geprüft:

- SMGW sendet Schema-valide Requests

Der Ablauf aller Negativtestfälle gestaltet sich wie folgt:

- Der Webservice-Benutzer SMGW sendet einen gültigen Request an den Webservice-Anbieter SMGW Administrator.
- In Abhängigkeit vom verwendeten Dienst werden ggf. relevante Daten als XML-Struktur an das SMGW übergeben.
- Der SMGW Administrator sendet auf den gültigen Request eine ungültige Response.
- Das SMGW muss die ungültige Response abweisen und darf sie nicht verarbeiten.

In den Negativtestfällen wird u. a. folgender Punkt geprüft:

- Verhalten bei Schema-invaliden Responses (z. B. falsche XML-Struktur und Werte außerhalb des definierten Wertebereichs [Grenzwerte])

Ist in einem Request eine XML-Struktur vorhanden, so muss diese auf Schema-Validität (siehe XSD Schema Relation) und korrekte Inhaltskodierung (siehe XML Inhaltskodierung) geprüft werden. Weiterhin muss geprüft werden, dass die im Request enthaltenen dienstabhängigen Daten CMS verschlüsselt vorliegen. Die jeweilige Prüfung kann bei den Negativtestfällen entfallen, die das Verhalten bei Schema-Invalidität bzw. falscher Inhaltskodierung testen.

Besonderheiten der verschiedenen Szenarien bzw. Abweichungen von dem oben beschriebenen Vorgehen werden in den entsprechenden Kapiteln beschrieben.

4.1.2.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	C	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	A	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	ja	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	A	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	A	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 79: Bewertungskriterien für WAF2: Zugriff auf Dienste beim SMGW Administrator

4.1.2.2 Zeitsynchronisation

Um nachzuweisen, dass die Zeitsynchronisation tatsächlich durchgeführt wird, muss die gesetzliche Zeit (an dem/den Zeitservern des SMGW-Admin) manipuliert werden. Beim nächsten Synchronisationsversuch muss das SMGW verschiedene Aktionen ausführen. Ist die Zeitabweichung innerhalb des erlaubten Zeitabweichungswertes, muss überprüft werden, dass das SMGW:

- eine Synchronisation durchführt und
- im Endverbraucherlog einen Hinweis über die vorgenommene Änderung einfügt.

Ist die Zeitabweichung und/oder die RTT höher als der erlaubte Wert, dann muss geprüft werden, dass

keine Synchronisation im SMGW durchgeführt wird, ab dem Zeitpunkt eingehende Messwerte gekennzeichnet werden und ein Eintrag im Eichlog erfolgt.

Durch Herabsetzung der Warnschwelle kann provoziert werden, dass ein Alarm des SMGW-Admin und ein Eintrag ins eichtechnische Log erfolgen sollte. Außerdem muss geprüft werden, dass durch einen Spannungsausfall die Systemzeit dennoch nicht abweicht (Absicherung durch Gangreserve). Durch eine gleichzeitige Manipulation der gesetzlichen Zeit (an dem/den Zeitservern des SMGW-Admin) kann die Resynchronisation nach Wiederinbetriebnahme getestet werden.

4.1.2.2.1 Testeingangskriterien, Abhängigkeiten

Alle Protokolltests müssen bestanden sein.

4.1.2.2.2 Testdaten

Ein registrierter Zähler muss Daten an das SMGW liefern, die dann entsprechend als gültig oder ungültig gekennzeichnet werden müssen.

4.1.2.2.3 Hinweise zu möglichen Testwerkzeugen (informativ)

-

4.1.2.3 Firmware Download

Das SMGW kann einen Dienst beim SMGW Administrator nutzen, um neue Firmware herunterzuladen. Dies darf nur auf Befehl des SMGW Administrators erfolgen. Ein Soft- oder Firmwareupdate von anderen Parteien darf nicht möglich sein. Um diese Funktionalität zu testen, werden Positiv- und Negativtestfälle erstellt.

In den Positivtestfällen sendet der Webservice-Benutzer SMGW Administrator bzw. SMGW gültige Requests an den Webservice-Anbieter SMGW bzw. SMGW Administrator. Das SMGW / der SMGW Administrator muss den gültigen Request verarbeiten. Das SMGW / der SMGW Administrator antwortet anschließend mit einer gültigen Response. Folgende Dienste werden genutzt und decken die Funktionalitäten entsprechend ab:

Dienst	Funktionalität
Notify (Event)	Firmware Download initiieren
Get	Firmware anfordern und downloaden

Tabelle 80: Dienst und Funktionalität

Bei den Negativtestfällen werden gültige Requests von nicht berechtigten Webservice-Benutzern (EMT, Letztverbraucher, Servicetechniker) zur Initiierung des Firmware Downloads an den Webservice-Anbieter SMGW gesendet. Das SMGW muss diese Requests wegen fehlender Berechtigung mit einem entsprechenden Fehlercode abweisen.

4.1.2.3.1 Testeingangskriterien, Abhängigkeiten

Bevor die Tests zum Firmware Download im WAF2 erfolgen können, müssen alle Protokolltests, die Tests zum WAF1 und der Test des SecMods erfolgreich abgeschlossen worden sein.

4.1.2.3.2 Testdaten

Die im Request gesendeten Daten müssen den Schemata [XSD-COD] und [XSD-COR] entsprechen und mittels CMS verschlüsselt und signiert sein.

4.1.2.3.3 Hinweise zu möglichen Testwerkzeugen (informativ)

Für den Test können zum Beispiel folgende Tools eingesetzt werden:

- Smartbear SoapUI
- Parasoft Virtualize

4.1.2.4 Auslieferung von tarifierten Messwerten oder Netzzustandsdaten

Das SMGW muss nach [BSI TR-03109-1] folgende Funktionalität beim SMGW Administrator nutzen können:

- Übertragung von tarifierten Messwerten und Netzzustandsdaten an den SMGW Administrator

Um diese Funktionalität zu testen, werden Positivtestfälle erstellt. Auf Negativtestfälle kann verzichtet werden, da das SMGW als Webservice-Benutzer agiert, somit die Requests erzeugt und eine Manipulation derer nicht möglich ist. Eine Manipulation der Response ist möglich, allerdings wird das Verhalten bei falschen Werten über die entsprechenden Testfälle im Protokolltest (z. B. HTTP Verben, HTTP Header-Felder, HTTP-Status-Codes) bereits geprüft.

In den Positivtestfällen wird folgender Dienst genutzt und deckt die Funktionalitäten entsprechend ab:

Dienst	Funktionalität
Create	Messwerte bzw. Netzzustandsdaten an den SMGW Administrator übergeben

Tabelle 81: Dienst und Funktionalität

4.1.2.4.1 Testeingangskriterien, Abhängigkeiten

Bevor die Tests zur Auslieferung von tarifierten Messwerten oder Netzzustandsdaten im WAF2 erfolgen können, müssen alle Protokolltests, die Tests zum WAF1 und der Test des SecMods erfolgreich abgeschlossen worden sein. Der SMGW Administrator muss sich mit dem SMGW verbinden können und er muss mit einem gültigen Zertifikat und seiner Kommunikationsadresse im SMGW eingerichtet sein.

4.1.2.4.2 Testdaten

Für die Tests zur Auslieferung von tarifierten Messwerten oder Netzzustandsdaten müssen folgende Testdaten vorhanden sein:

- Mehrere Letztverbraucher müssen im SMGW vorhanden sein. (Es könnten z. B. die in der Mandatenverwaltung angelegten Letztverbraucher genutzt werden.)
- Mehrere Zähler müssen im SMGW vorhanden sein. (Es könnten z. B. die in der Geräteverwaltung angelegten Zähler genutzt werden.)
- Es müssen verschiedene tarifierte Messwerte für verschiedene Zähler für die Auslieferung vorhanden sein.
- Es müssen verschiedene Auswertungsprofile mit verschiedenen Versandzeitpunkten vorhanden sein.
- Es müssen verschiedene Kommunikationsprofile für die Kommunikation mit den EMT vorhanden sein.

4.1.2.4.3 Hinweise zu möglichen Testwerkzeugen (informativ)

Für den Test können zum Beispiel folgende Tools eingesetzt werden:

- Smartbear SoapUI
- Parasoft Virtualize

4.1.3 WAF3: Alarmierung und Benachrichtigung

Während des Betriebs des SMGW können unerwartete Ereignisse oder Fehlersituationen auftreten, die zur Analyse und weiteren Bearbeitung an den SMGW Administrator gemeldet werden müssen. Ebenso kann das SMGW regelmäßig Benachrichtigungen an den SMGW Administrator senden (z. B. jeden Tag eine „Alive“ Nachricht). Damit das SMGW solche Nachrichten an den SMGW Administrator übermitteln kann, muss das SMGW einen Dienst beim SMGW Administrator aufrufen, der die Zustellung solcher Ereignisse durch das SMGW ermöglicht. Um diese Funktionalität zu testen, werden Positivtestfälle erstellt und es wird das Kommunikationsszenario „ADMIN-SERVICE“ genutzt. Auf Negativtestfälle kann verzichtet werden, da das

SMGW als Webservice-Benutzer agiert, somit die Requests erzeugt und eine Manipulation derer nicht möglich ist. Eine Manipulation der Responses ist möglich, allerdings wird das Verhalten bei falschen Werten über die entsprechenden Testfälle im Protokolltest (z. B. HTTP Verben, HTTP Header-Felder, HTTP-Status-Codes) bereits geprüft.

Der Ablauf aller Positivtestfälle gestaltet sich wie folgt:

- Der Webservice-Benutzer SMGW sendet einen gültigen Request an den Webservice-Anbieter SMGW Administrator.
- In Abhängigkeit vom verwendeten Dienst werden ggf. relevante Daten als XML-Struktur an das SMGW übergeben.
- Der SMGW Administrator sendet eine gültige Response.
- Das SMGW muss die vom SMGW Administrator gesendete gültige Response verarbeiten.

In den Positivtestfällen wird u. a. geprüft:

- SMGW sendet Schema-valide Requests

Ist in einem Request eine XML-Struktur vorhanden, so muss diese auf Schema-Validität (siehe XSD Schema Relation) und korrekte Inhaltskodierung (siehe XML Inhaltskodierung) geprüft werden. Weiterhin muss geprüft werden, dass die im Request enthaltenen dienstabhängigen Daten CMS verschlüsselt vorliegen.

4.1.3.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	C	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	A	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	ja	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	B	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	A	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 82: Bewertungskriterien für WAF3: Alarmierung und Benachrichtigung

4.1.3.2 Tests

Folgender Dienst wird genutzt und deckt die Funktionalität entsprechend ab:

Dienst	Funktionalität
Notify (Event)	Zustellung von Ereignissen/Informationen

Tabelle 83: Dienst und Funktionalität

4.1.3.2.1 Testeingangskriterien, Abhängigkeiten

Bevor die Tests zur Alarmierung und Benachrichtigung im WAF3 erfolgen können, müssen alle Protokolltests, die Tests zum WAF1 und der Test des SecMods erfolgreich abgeschlossen worden sein. Der SMGW Administrator muss sich mit dem SMGW verbinden können und er muss mit einem gültigen Zertifikat und seiner Kommunikationsadresse im SMGW eingerichtet sein.

4.1.3.2.2 Testdaten

Für die Tests zur Alarmierung und Benachrichtigung müssen folgende Testdaten vorhanden sein:

- Es müssen verschiedene externe Ereignisse ausgelöst werden, die eine Alarmierung des SMGW Administrators bewirken.

4.1.3.2.3 Hinweise zu möglichen Testwerkzeugen (informativ)

Für den Test können zum Beispiel folgende Tools eingesetzt werden:

- Smartbear SoapUI
- Parasoft Virtualize

4.1.4 WAF4: Übertragung von Daten an den SMGW Administrator

Die Übertragung von Daten an den SMGW Administrator muss durch den Aufruf eines Dienstes beim SMGW Administrator erfolgen und fällt somit in die Kategorie „ADMIN-SERVICE“. Auf Testfälle kann verzichtet werden, da dies über die Anwendungsfälle WAF2 und WAF3 abgedeckt wird. Sind alle Positivtestfälle der WAF2 und WAF3 bestanden, gilt die MUSS-Anforderung als bestanden.

4.1.4.1 Testeingangskriterien, Abhängigkeiten

Die Testfälle der Anwendungsfälle WAF2 und WAF3 müssen bestanden sein.

4.1.4.2 Testdaten

Es werden für dieses Szenario keine Testdaten benötigt.

4.1.4.3 Hinweise zu möglichen Testwerkzeugen (informativ)

-

4.1.5 WAF5: Übertragung von Daten an externe Marktteilnehmer

Der WAF5 umfasst viele Anforderungen. Aus diesem Grund wird dieser Anwendungsfall in verschiedene Szenarien eingeteilt. Sind alle Szenarien bestanden, gilt auch die Anforderung „Daten an eine

Dienstschnittstelle beim externen Marktteilnehmer übergeben“ als bestanden. Alle Szenarien nutzen das Kommunikationsszenario „INFO-REPORT“.

Der Ablauf aller Positivtestfälle gestaltet sich wie folgt:

- Der Webservice-Benutzer SMGW sendet einen gültigen Request an den Webservice-Anbieter SMGW Administrator.
- In Abhängigkeit vom verwendeten Dienst werden ggf. relevante Daten als XML-Struktur an das SMGW übergeben.
- Der SMGW Administrator sendet eine gültige Response.
- Das SMGW muss die vom SMGW Administrator gesendete gültige Response verarbeiten.

In den Positivtestfällen wird u. a. geprüft:

- SMGW sendet Schema-valide Requests

Ist in einem Request eine XML-Struktur vorhanden, so muss diese auf Schema-Validität (siehe XSD Schema Relation) und korrekte Inhaltskodierung (siehe XML Inhaltskodierung) geprüft werden. Weiterhin muss geprüft werden, dass die im Request enthaltenen dienstabhängigen Daten CMS verschlüsselt vorliegen.

Besonderheiten der verschiedenen Szenarien bzw. Abweichungen von dem oben beschriebenen Vorgehen werden in den entsprechenden Kapiteln beschrieben.

4.1.5.1 Testelementbewertung

Bewertungs-ebene	**Kriterium**	**Bewertungs-maßstab**	**Bewertungs-ergebnis**	**Erläuterung / Begründung**
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	C	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	A	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	ja	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	B	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	A	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 84: Bewertungskriterien für WAF5: Übertragung von Daten an externe Marktteilnehmer

4.1.5.2 Turnusmäßige Auslieferung von tarifierten Messwerten

Das SMGW muss nach [BSI TR-03109-1] folgende Funktionalität bei einem EMT nutzen können:

- regelmäßige Auslieferung von abrechnungsrelevanten tarifierten Messwerten an einen externen Marktteilnehmer gemäß eines Auswertungs- und eines Kommunikationsprofils

Um diese Funktionalität zu testen, werden Positivtestfälle erstellt. Auf Negativtestfälle kann verzichtet werden, da das SMGW als Webservice-Benutzer agiert, somit die Requests erzeugt und eine Manipulation derer nicht möglich ist. Eine Manipulation der Response ist möglich, allerdings wird das Verhalten bei falschen Werten über die entsprechenden Testfälle im Protokolltest (z. B. HTTP Verben, HTTP Header-Felder, HTTP-Status-Codes) bereits geprüft.

Folgender Dienst wird genutzt und deckt die Funktionalität entsprechend ab:

Dienst	Funktionalität
Create	Auslieferung tarifierter Messwerte

Tabelle 85: Dienst und Funktionalität

4.1.5.2.1 Testeingangskriterien, Abhängigkeiten

Bevor die Tests zur Turnusmäßige Auslieferung von tarifierten Messwerten im WAF5 erfolgen können, müssen alle Protokolltests, die Tests zum WAF1 und der Test des SecMods erfolgreich abgeschlossen worden sein. Der SMGW Administrator muss sich mit dem SMGW verbinden können und er muss mit einem gültigen Zertifikat und seiner Kommunikationsadresse im SMGW eingerichtet sein.

4.1.5.2.2 Testdaten

Für die Tests zur Turnusmäßige Auslieferung von tarifierten Messwerten müssen folgende Testdaten vorhanden sein:

- Mehrere Letztverbraucher müssen im SMGW vorhanden sein (man könnte z. B. die in der Mandatenverwaltung angelegten Letztverbraucher nutzen).
- Mehrere Zähler müssen im SMGW vorhanden sein. (Es könnten z. B. die in der Geräteverwaltung angelegten Zähler genutzt werden.)
- Es müssen verschiedene Messwerte für verschiedene Zähler für die Auslieferung vorhanden sein. (Es könnten z. B. die in LAF2: Abruf/Empfang von Messwerten gelieferten Messwerte genutzt werden.)
- Es müssen verschiedene Auswertungs- und Kommunikationsprofile für verschiedene EMT im SMGW vorhanden sein. (Es könnten z. B. die in der Profilverwaltung angelegten Profile genutzt werden.)

4.1.5.2.3 Hinweise zu möglichen Testwerkzeugen (informativ)

Für den Test können zum Beispiel folgende Tools eingesetzt werden:

- Smartbear SoapUI
- Parasoft Virtualize

4.1.5.3 Turnusmäßige Netzzustandsdatenauslieferung

Das SMGW muss nach [BSI TR-03109-1] folgende Funktionalität bei einem EMT nutzen können:

- regelmäßige Auslieferung von Messwerten zum Netzzustand an einen externen Marktteilnehmer gemäß eines Auswertungs- und eines Kommunikationsprofils

Um diese Funktionalität zu testen, werden Positivtestfälle erstellt. Auf Negativtestfälle kann verzichtet werden, da das SMGW als Webservice-Benutzer agiert, somit die Requests erzeugt und eine Manipulation derer nicht möglich ist. Eine Manipulation der Response ist möglich, allerdings wird das Verhalten bei falschen Werten über die entsprechenden Testfälle im Protokolltest (z. B. HTTP Verben, HTTP Header-Felder, HTTP-Status-Codes) bereits geprüft.

Folgender Dienst wird genutzt und deckt die Funktionalität entsprechend ab:

Dienst	Funktionalität
Create	Auslieferung von Messwerten zum Netzzustand

Tabelle 86: Dienst und Funktionalität

4.1.5.3.1 Testeingangskriterien, Abhängigkeiten

Bevor die Tests zur Turnusmäßigen Netzzustandsdatenauslieferung im WAF5 erfolgen können, müssen alle Protokolltests, die Tests zum WAF1 und der Test des SecMods erfolgreich abgeschlossen worden sein. Der SMGW Administrator muss sich mit dem SMGW verbinden können und er muss mit einem gültigen Zertifikat und seiner Kommunikationsadresse im SMGW eingerichtet sein.

4.1.5.3.2 Testdaten

Für die Tests zur Turnusmäßige Netzzustandsdatenauslieferung müssen folgende Testdaten vorhanden sein:

- Mehrere Letztverbraucher müssen im SMGW vorhanden sein. (Es könnten z. B. die in der Mandatenverwaltung angelegten Letztverbraucher genutzt werden.)
- Mehrere Zähler müssen im SMGW vorhanden sein. (Es könnten z. B. die in der Geräteverwaltung angelegten Zähler genutzt werden.)
- Es müssen verschiedene Messwerte für verschiedene Zähler für die Auslieferung vorhanden sein. (Es könnten z. B. die in LAF2: Abruf/Empfang von Messwerten gelieferten Messwerte genutzt werden.)
- Es müssen verschiedene Auswertungs- und Kommunikationsprofile für verschiedene EMT im SMGW vorhanden sein. (Es könnten z. B. die in der Profilverwaltung angelegten Profile genutzt werden.)
- Es muss eines der in der [BSI TR-03109-1] definierten Ereignisse ausgelöst werden. (Die Auslösung des Ereignisses kann z. B. durch den Testtreiber erfolgen.)

4.1.5.3.3 Hinweise zu möglichen Testwerkzeugen (informativ)

Für den Test können zum Beispiel folgende Tools eingesetzt werden:

- Smartbear SoapUI
- Parasoft Virtualize

4.1.5.4 Spontane Messwertauslesung

Das SMGW muss nach [BSI TR-03109-1] folgende Funktionalität bei einem EMT nutzen können:

- spontane Auslieferung von Messwerten an einen externen Marktteilnehmer gemäß eines entsprechenden Auswertungs- und eines Kommunikationsprofils

Um diese Funktionalität zu testen, werden Positivtestfälle erstellt. Auf Negativtestfälle kann verzichtet werden, da das SMGW als Webservice-Benutzer agiert, somit die Requests erzeugt und eine Manipulation derer nicht möglich ist. Eine Manipulation der Response ist möglich, allerdings wird das Verhalten bei

falschen Werten über die entsprechenden Testfälle im Protokolltest (z. B. HTTP Verben, HTTP Header-Felder, HTTP-Status-Codes) bereits geprüft.

Folgender Dienst wird genutzt und deckt die Funktionalität entsprechend ab:

Dienst	Funktionalität
Create	Auslieferung spontan ausgelesener Messwerte

Tabelle 87: Dienst und Funktionalität

4.1.5.4.1 Testeingangskriterien, Abhängigkeiten

Bevor die Tests zur spontanen Messwertauslesung im WAF5 erfolgen können, müssen alle Protokolltests, die Tests zum WAF1 und der Test des SecMods erfolgreich abgeschlossen worden sein. Der SMGW Administrator muss sich mit dem SMGW verbinden können und er muss mit einem gültigen Zertifikat und seiner Kommunikationsadresse im SMGW eingerichtet sein.

4.1.5.4.2 Testdaten

Für die Tests zur Turnusmäßige Auslieferung von tarifierten Messwerten müssen folgende Testdaten vorhanden sein:

- Mehrere Letztverbraucher müssen im SMGW vorhanden sein. (Es könnten z. B. die in der Mandatenverwaltung angelegten Letztverbraucher genutzt werden.)
- Mehrere Zähler müssen im SMGW vorhanden sein. (Es könnten z. B. die in der Geräteverwaltung angelegten Zähler genutzt werden.)
- Es müssen verschiedene Messwerte für verschiedene Zähler für die Auslieferung vorhanden sein. (Es könnten z. B. die in LAF2: Abruf/Empfang von Messwerten gelieferten Messwerte genutzt werden.)
- Es müssen verschiedene Auswertungs- und Kommunikationsprofile für verschiedene EMT im SMGW vorhanden sein. (Es könnten z. B. die in der Profilverwaltung angelegten Profile genutzt werden.)

4.1.5.4.3 Hinweise zu möglichen Testwerkzeugen (informativ)

Für den Test können zum Beispiel folgende Tools eingesetzt werden:

- Smartbear SoapUI
- Parasoft Virtualize

4.1.6 WAF6: Kommunikation EMT mit CLS

Das SMGW muss Anwendungsfälle zur Kommunikation eines externen Marktteilnehmers mit einem CLS Gerät unter Nutzung der TLS Proxy Funktionalität des SMGW unterstützen. Dieser Anwendungsfall wird durch den Anwendungsfall HAF3 im Kapitel 4.2 HAN abgedeckt. Ist der Anwendungsfall HAF3 bestanden, gilt auch der Anwendungsfall WAF6 als bestanden.

4.1.6.1 Testeingangskriterien, Abhängigkeiten

Alle Testfälle zum HAF3 im Kapitel 4.2 HAN müssen bestanden sein.

4.1.6.2 Testdaten

Es werden für dieses Szenario keine Testdaten benötigt.

4.1.6.3 Hinweise zu möglichen Testwerkzeugen (informativ)

-

4.1.7 WAF7: Wake-Up Service

Das SMGW muss den Wake-Up Service implementieren. Dieses Szenario wird über die Wake-Up-Protokolltests ausreichend abgedeckt. Ein separater Test der Funktionalität ist damit nicht notwendig. Sind alle Testfälle im Wake-Up-Protokolltest bestanden, gilt auch dieses Szenario als bestanden.

4.1.7.1 Testeingangskriterien, Abhängigkeiten

Alle Wake-Up-Protokolltests müssen bestanden sein.

4.1.7.2 Testdaten

Es werden für dieses Szenario keine Testdaten benötigt.

4.1.7.3 Hinweise zu möglichen Testwerkzeugen (informativ)

-

4.1.8 Personalisierung

In diesem Kapitel wird beschrieben, wie die Aspekte der Personalisierung, im Sinne der initialen Konfiguration des SMGW durch den SMGW-Admin sowie die Installation der Betriebsschlüssel (vgl. [BSI TR-03109-1], Anlage 6, Kapitel 2.3.3), getestet werden.

Die Personalisierung beinhaltet insbesondere die initiale Konfiguration des SMGW durch den SMGW-Admin und die Installation der Betriebsschlüssel. Die ausführliche Beschreibung der Vorgänge erfolgt in [BSI TR-03109-1/AVI].

4.1.8.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	ja	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	B	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	B	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 88: Bewertungskriterien für WAN / Personalisierung

4.1.8.2 Test

Der initiale Aufbau der Verbindung zwischen SMGW-Admin und SMGW erfolgt über eine TLS gesicherte Verbindung wie in 3.2.1 beschrieben, jedoch mit den bereits in das SMGW eingebrachten vorläufigen WAN-TLS Gateway-Schlüsseln (`GW_WAN_TLS_PRV_PRE` und `GW_WAN_TLS_PUB_PRE`) und dem zugehörigen Zertifikat (`GW_WAN_TLS_CRT_PRE`). Im Test wird ermittelt, ob diese initial eingebrachten Schlüssel und Zertifikate denselben Anforderungen genügen, wie sie im Normalbetrieb gefordert sind. Dies wird im Kontext von Blackbox-Tests durchgeführt, weshalb nur Tests zu Parametern formuliert sind, die auch mithilfe des Blackbox-Testverfahrens überprüft werden können. Die Schlüssel und das Zertifikat des SMGW-Admin liegen diesem bereits vor und sind bis zur ROOT-CA geprüft. Diese müssen in der Testumgebung vorhanden sein (Admin Test-Schlüssel und Zertifikate, welche ebenfalls signiert sind), um eine Verbindung zum SMGW über einen TLS-Kanal aufbauen zu können.

Ist dieser initiale TLS-Kanal aufgebaut, wird geprüft, ob der SMGW-Admin im SMGW die Generierung von neuen Schlüsselpaaren veranlassen kann. Hierfür spricht das SMGW intern das SecMod an. Die somit neu generierten Schlüssel (`GW_WAN_TLS_PRV, GW_WAN_TLS_PUB, GW_WAN_SIG_PRV, GW_WAN_SIG_PUB, GW_WAN_ENC_PRV, GW_WAN_ENC_PUB`) werden auf Konformität mit den Anforderungen aus [BSI TR-03109-1] und [BSI TR-03109-3] überprüft. Hierfür werden Nachrichten mit der Testumgebung ausgetauscht und die Nachrichten entsprechend den Vorgaben aus [BSI TR-03109-1] und [BSI TR-03109-3] mit den jeweiligen Algorithmen zu entschlüsseln. Ist dies erfolgreich, so kann davon ausgegangen werden, dass die erstellten Schlüsselpaare [BSI TR-03109-1]-konform erzeugt wurden.

Danach wird geprüft, ob die Public Keys (GW_WAN_TLS_PUB, GW_WAN_SIG_PUB, GW_WAN_ENC_PUB) über die WAN-Schnittstelle exportiert werden können.

Sind die vorherigen Schritte erfolgreich getestet worden, so werden Zertifikatsanfragen an die Test-PKI für die neuen Betriebszertifikate zu den neuen SMGW-Schlüsseln gesendet. Als Antwort auf diese Anfragen erhält der SMGW-Admin von der Test-PKI die Betriebszertifikate, welche er über den TLS-Kanal in das SMGW einbringt und dort speichert. War der Import erfolgreich, so wird der TLS-Kanal zwischen SMGW und SMGW-Admin geschlossen. Testfälle werden hier so konzipiert, dass sichergestellt wird, dass das SMGW eine Funktionalität bietet, mithilfe derer ein SMGW-Admin in der Lage ist Zertifikate in das SMGW einzuspielen.Werden die genannten Tests erfolgreich abgeschlossen, befindet sich das SMGW im personalisierten Zustand und beim Neuaufbau der TLS-Verbindung im Normalbetrieb.

Diese Überprüfung stellt die Grundlage für spätere TLS- und Verbindungstests des SMGW dar.

4.1.8.3 Testeingangskriterien, Abhängigkeiten

Das SecMod wurde korrekt in das SMGW integriert und ist funktionstüchtig.

Der SMGW-Admin muss sich gegenüber dem SecMod mithilfe des SMGW-Admin-Schlüssels authentisieren können.

Die Zertifikate aus der Test-PKI sind bis zur ROOT-CA gültig.

4.1.8.4 Testdaten

Schlüssel: GW_WAN_TLS_PRV_PRE und GW_WAN_TLS_PUB_PRE

Zertifikat: GW_WAN_TLS_CRT_PRE

4.1.8.5 Hinweise zu möglichen Testwerkzeugen (informativ)

Zum Testen der SSL-Parameter kann auf die Programme „sslscan“ (Test des SMGW als TLS-Server) sowie „openssl“ (Test des SMGW als TLS-Client bzw. TLS-Server) zurückgegriffen werden.

Möglich wäre auch die Entwicklung eigener Testsoftware unter Verwendung vorhandener Bibliotheken (z. B. openSSL, GnuTLS)

Inwiefern alle Anforderungen der TR von diesen Programmen unterstützt werden und alle Testfälle mit diesen Programmen durchgeführt werden können, muss im Rahmen des Aufbaus der Testinfrastruktur geprüft werden.

Name	Hersteller	Quelle	Testfokus
sslscan (fork von DinoTools)	Ian Ventura-Whiting, Jacob Appelbaum, DinoTools	https://github.com/DinoTools/sslscan	Cipher Suites, die das SMGW als TLS-Server anbietet
TLSSLed	Raul Siles, Taddong SL	http://www.taddong.com/en/lab.html	Cipher Suites, die das SMGW als TLS-Server anbietet
diverse SSL Implementierungen	verschiedene	https://en.wikipedia.org/wiki/Comparison_of_TLS_Implementations	Cipher Suites, die das SMGW als TLS-Server bzw. TLS-Client anbietet; verschlüsselte Kommunikation

Tabelle 89: Information Testwerkzeuge Personalisierung

4.2 HAN

An der HAN-Schnittstelle sind die folgenden drei Anwendungsfälle zu implementieren und somit auch zu testen:

- HAF1 – Bereitstellung von Daten für den Letztverbraucher – IF_GW_CON
- HAF2 – Bereitstellung von Daten für den Service-Techniker – IF_GW_SRV
- HAF3 – Transparenter Kommunikationskanal zwischen CLS und EMT – IF_GW_CLS

Die drei Anwendungsfälle nutzen die folgenden fünf Kommunikationsszenarien, die vom SMGW unterstützt werden MÜSSEN:

- HKS1: Bidirektionale Kommunikation im HAN bei Authentifizierung mittels HAN-Zertifikaten
- HKS2: Bidirektionale Kommunikation im HAN bei Authentifizierung mittels eindeutiger Kennung und Passwort
- HKS3: Transparenter Kanal initiiert durch CLS
- HKS4: Transparenter Kanal initiiert durch EMT
- HKS5: Transparenter Kanal initiiert durch SMGW

Da die Testeingangskriterien, Werkzeuge und Testdaten der einzelnen Anwendungsfälle ähnlich zueinander sind, werden diese am Ende des Kapitels zusammengefasst und nicht einzelnen betrachtet.

4.2.1 HAF1: Bereitstellung von Daten für den Letztverbraucher

Zur Prüfung von HAF1 wird getestet, dass sich registrierte Letztverbraucher per HAN-Zertifikat (HKS1) und per Kennung und Passwort anmelden und anschließend die folgenden Daten abrufen können:

- Datum und Systemzeit des SMGW
- Aktuelle Zählerstände in kWh oder m³ der am SMGW angeschlossenen und dem Letztverbraucher zugeordneten Zähler.
- Aktuelle Tarifstufe je Auswertungsprofil.
- Historische Daten gemäß Energieeffizienzrichtlinie [EER]

  Dabei müssen Verbrauchs- sowie Einspeisewerte für die folgenden Zeiträume bereitgestellt werden:

  - die letzten 7 Tage, Tag für Tag
  - die letzte Woche (aggregiert)
  - das letzte Jahr (aggregiert)
  - mindestens die letzten 15 Monate (Monat für Monat aggregiert)
- Messwerte der letzten 24h in einer Granularität, wie sie das SMGW vom Zähler erfasst und zur Aktualisierung der abgeleiteten Register verwendet.
- Daten aus dem Letztverbraucher-Log

Dabei ist darauf zu achten, dass der jeweilige Letztverbraucher nur Zugriff auf seine Daten hat. Weiterhin ist zu prüfen, dass nur Letztverbraucher mit korrekten Zugangsdaten bzw. korrektem Zertifikat Zugriff auf Daten der IF_GW_CON erhalten. Weiterhin muss getestet werden, dass die ausgelesenen Daten aus dem Letztverbraucher-Log in einer XML-Struktur schemakonform bereitgestellt werden und folgende Informationen enthalten:

- record_number

- date time
- level
- event_type
- subject_identity
- outcome
- message
- user_identity
- destination
- evidence

4.2.1.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	ja	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	ja	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	C	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	A	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	Details sind im Rahmen AP2 und 3 zu prüfen.

Tabelle 90: Bewertungskriterien für HAF1: Bereitstellung von Daten für den Letztverbraucher

4.2.2 HAF2: Bereitstellung von Daten für den Service-Techniker

Um die Bereitstellung von Daten für den Servicetechniker zu prüfen, wird getestet, ob sich ein am SMGW registrierter Techniker mit seinem HAN-Zertifikat an der Schnittstelle IF_GW_SRV authentifizieren kann und danach alle Daten des Systemlogs und weitere Diagnose-Informationen abrufen kann. Es ist weiterhin zu prüfen, dass der Servicetechniker keinen Zugriff auf die Daten der Letztverbraucher hat und keine personenbezogenen Daten abrufen kann. Darüber hinaus ist zu testen, dass ein Login mit dem HAN-Zertifikat des Servicetechnikers nicht an der Schnittstelle des Endverbrauchers möglich ist.

4.2.2.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	A	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	ja / nein	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	B	-
	Informativ: bekannte Sicherheitsrisiken und Angriffsszenarien	Auswahl (ja oder nein)	nein	Anmerkung: Es sind Angriffe über die optischen Schnittstellen auf Zähler in Ländern bekannt, die bereits einen Smart Meter Rollout durchgeführt haben. Da die Angriffsverfahren auf der dort eingesetzte Zählertechnologie basieren, ist die Übertragung auf die deutschen Verhältnisse relativ zu sehen.
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	A	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	Details sind im Rahmen AP2 und 3 zu prüfen.

Tabelle 91: Bewertungskriterien für HAF2: Bereitstellung von Daten für den Service-Techniker

4.2.3 HAF3: Transparenter Kommunikationskanal zwischen CLS und EMT

Im Anwendungsfall HAF3 geht es um die Bereitstellung einer Proxy-Funktion zwischen Controllable Local Systems (CLS) und externen Marktteilnehmern (EMT) im WAN. Dabei wird geprüft, ob ein transparenter Kanal vom CLS, vom EMT und vom SMGW aufgebaut und anschließend genutzt werden kann. Dabei wird darauf geachtet, dass der Kanal für den EMT bzw. das CLS transparent ist, die Verbindung nach SOCKSv5 etabliert wird und die Authentifizierung durch die korrekten Zertifikate erfolgt. Durch Negativtests wird sichergestellt, dass keine anderen Zertifikate verwendet werden können.

4.2.3.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	A	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	A, wenn über die CLS Erzeuger/Lasten angesteuert werden können, deren Schalt-Leistung eine Auswirkung auf die Frequenzregelung/-stabilität haben und deshalb der Schaltzeitpunkt beim BKV im Fahrplan vermerkt sein sollte.
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	ja	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	B	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	A	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	Details sind im Rahmen AP2 und 3 zu prüfen.

Tabelle 92: Bewertungskriterien für HAF3: Transparenter Kommunikationskanal zwischen CLS und EMT

4.2.4 Testeingangskriterien, Abhängigkeiten

Um die Tests für die Anwendungsfälle HAF1 und HAF2 durchführen zu können, ist es notwendig, dass die Protokollprüfungen zu HAN bis auf die Tests zu SOCKSv5 komplett bestanden wurden. Die Prüfung des HAF3 erfordert dazu, dass die Tests zu SOCKSv5 bestanden wurden und dass die WAN-Kommunikation funktioniert, um die Verbindung zum EMT prüfen zu können.

4.2.5 Testdaten

Zum Prüfen der Anwendungsfälle HAF1 und HAF2 müssen entsprechende Daten, also Einträge in den Logs, Messwerte und Konfigurationsprofile vorher in das SMGW eingebracht werden. Dazu könne in vielen Fällen die Testfälle aus den Bereichen WAN und LMN genutzt werden.

Bei dem Anwendungsfall HAF3 wird hauptsächlich geprüft, dass ein transparenter Kommunikationskanal aufgebaut wird. Die dazu notwendigen Zertifikate werden dabei von der Prüfumgebung generiert und in das SMGW eingebracht.

Um zu prüfen, dass ein aufgebauter Kanal transparent ist, werden beliebige, z.B.zufällig generierte Daten übertragen und auf der Gegenstelle geprüft, dass diese unverändert ankommen.

4.2.6 Hinweise zu möglichen Testwerkzeugen (informativ)

Da für die Schnittstellen `IF_GW_CLS` und `IF_GW_SRV` keine konkreten Protokolle definiert sind, kann nicht auf bestimmte Testwerkzeuge verwiesen werden.

Zur Prüfung der Transparenz des aufgebauten Kanals ist ein Testwerkzeug einzusetzen, welches Daten über eine TLS-gesicherte Verbindung senden und gleichzeitig auf einer zweiten Verbindung empfangen und vergleichen kann.

4.3 LMN

Im LMN müssen die Anwendungsfälle LAF1 – LMN-Zählerverwaltung und LAF2 – Abruf/Empfang von Messwerten unterstützt werden. Die Zählerverwaltung teilt sich in die Bereiche Registrierung bzw. Konfiguration und Schlüssel-/Zertifikatsmanagement. Beim Zertifikatsmanagement müssen die folgenden Fälle unterstützt werden.

- Generieren von öffentlichen und privaten Schlüsseln für LMN Zähler
- Generieren von selbst-signierten TLS Zertifikaten durch das SMGW
- Einbringen und Erneuern der TLS Zertifikate für bidirektional angeschlossene Zähler
- Austausch des jeweiligen zählerindividuellen „Master“-Schlüssels für die symmetrische Verschlüsselung bei drahtlos, bidirektional angeschlossenen Zählern

Die Zähler können entweder bidirektional nach LKS1 oder unidirektional nach LKS2 mit dem SMGW kommunizieren. Dabei wird die unidirektionale Kommunikation hauptsächlich für das Liefern von Messwerten an das SMGW genutzt.

Die an den Tests beteiligten Zähler werden von der Testumgebung simuliert.

Da die Testeingangskriterien, Werkzeuge und Testdaten der einzelnen Anwendungsfälle ähnlich zueinander sind, werden diese am Ende des Kapitels zusammengefasst und nicht einzelnen betrachtet.

4.3.1 LAF1: LMN Zählerverwaltung

In den Tests zur Zählerverwaltung wird geprüft, ob im SMGW durch den SMGW Administrator Zähler registriert, konfiguriert und einem Letztverbraucher zugeordnet werden können. Weiterhin wird überprüft, dass auf Anforderung des SMGW Administrators Schlüssel und Zertifikate für die Kommunikation mit Zählern erstellt, verteilt, aktiviert, deaktiviert und gelöscht werden können. Dabei wird weiterhin geprüft, dass die beim Zertifikatsmanagement vorgeschriebenen Fälle korrekt umgesetzt sind. Es ist ausschließlich das Kommunikationsszenario LKS1 zu unterstützen, da alle Anfragen eine direkte Antwort erfordern.

4.3.1.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	ja	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	A	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	A	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	Details sind im Rahmen AP2 und 3 zu prüfen.

Tabelle 93: Bewertungskriterien für LAF1: LMN Zählerverwaltung

4.3.2 LAF2: Abruf/Empfang von Messwerten

Messwerte können entweder periodisch und unaufgefordert vom Zähler an das SMGW geliefert werden oder werden vom SMGW einzeln vom Zähler angefordert. Diese Einzelabrufe können bei Bedarf auch periodisch durchgeführt werden.

Das periodische Zuliefern von Messwerten kann unidirektional nach LKS2 erfolgen. Einzelabfragen erfordern dagegen immer eine bidirektionale Verbindung (LKS1).

Es wird geprüft, ob die unidirektionalen Messwerte korrekt anhand von im Vorfeld einzubringenden Regelwerken bzw. Zählerprofilen verarbeitet und in die entsprechenden abgeleiteten Wertelisten eingetragen werden. Auf die gleiche Weise wird auch der Einzelabruf von Messwerten getestet. Dabei wird durch Negativtests mit Messwerten aus den falschen OBIS Value Groups sichergestellt, dass nur untarifierte Messwerte verarbeitet werden.

Weiterhin wird geprüft, dass die Zählerstände von mehreren Zählern erfasst werden können und die aktuellen Messgrößen durch das SMGW vorgehalten werden. Dabei wird auch geprüft, dass das SMGW korrekt mit fehlerhaften Messwerten umgeht.

4.3.2.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	ja	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	C	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	A	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	Details sind im Rahmen AP2 und 3 zu prüfen.

Tabelle 94: Bewertungskriterien für LAF2: Abruf/Empfang von Messwerten

4.3.3 Testeingangskriterien, Abhängigkeiten

Um die Tests der Anwendungsfälle im LMN durchführen zu können, müssen die Tests der Schnittstellen im LMN bestanden sein. Dazu ist es für die vorbereitende Einrichtung des SMGW und die Prüfung der Verhaltensweise notwendig, dass die Protokolle der WAN-Schnittstelle korrekt funktionieren.

4.3.4 Testdaten

Die Tests der LMN-Anwendungsfälle werden mit verschiedenen Testdatensätzen ausgeführt, um indirekt die Anforderungen zur Verarbeitung von Messwerten zu prüfen. Dazu werden mehrere verschiedene Konfigurationsprofile in das SMGW eingebracht. Insbesondere Zähler- und Auswertungsprofile sind in verschiedene Variationen notwendig. Da die Zähler von der Prüfumgebung simuliert werden, können zählerindividuelle Daten, wie die Geräte-ID oder die Schlüsseldaten in den verschiedenen Zählerprofilen fest definiert werden und brauchen nicht in jedem Testlauf einzeln festgelegt werden.

Die zu nutzenden Testdaten sind in den einzelnen Tests festgelegt.

4.3.5 Hinweise zu möglichen Testwerkzeugen (informativ)

Die Prüfung der LMN-Anwendungsfälle ist eng mit der Kommunikation zum Liefern der Daten bzw. dem Verarbeiten von Konfigurationsprofilen und Messwerten verknüpft. Dadurch kommen als Testwerkzeuge die gleichen Tools wie bei der Prüfung der oberen Schichten der Protokolle zum Senden und Empfangen von Nachrichten zum Einsatz. Durch die starke Individualisierung der Anforderungen an die Verarbeitung in Abhängigkeit zu den eingebrachten Konfigurationsprofilen sind zur Auswertung und Prüfung der Testergebnisse keine Standardtestwerkzeuge einsetzbar. Die entsprechenden Funktionen sind von der Prüfumgebung zur Verfügung zu stellen.

4.4 Schnittstellen-übergreifend: Anwendungsfälle Tarifierung

Die [BSI TR-03109-1] spezifiziert 13 Anwendungsfälle, kurz TAF genannt, für die Tarifierung, Bilanzierung und Netzzustandsdatenerhebung. Diese 13 Anwendungsfälle sind in der folgenden Tabelle dargestellt, gruppiert nach dem Auslöser im Regelwerk. Die TAF 11, 12 und 13 sind nur informativ in [BSI TR-03109-1]aufgeführt und werden nicht getestet.

Anwendungsfall		**Auslöser im Regelwerk**
TAF 1	Datensparsame Tarife	Internes Ereignis: Zeitpunkt
TAF 2	Zeitvariable Tarife	
TAF 7	Zählerstandsgangmessung	
TAF 8	Erfassung von Extremwerten	
TAF 3	Lastvariable Tarife	Internes Ereignis: Grenzwert
TAF 4	Verbrauchsvariable Tarife	
TAF 12	Prepaid Tarif (informativ)	
TAF 5	Ereignisvariable Tarife	Internes oder externes Ereignis
TAF 10	Abruf von Netzzustandsdaten	
TAF 6	Ablesung von Messwerten im Bedarfsfall	Externes Ereignis
TAF 9	Abruf der Ist-Einspeisung	
TAF 11	Steuerung von unterbrechbaren Verbrauchseinrichtungen und Erzeugungsanlagen (informativ)	
TAF 13	Bereitstellung von Messwertsätzen zur Visualisierung für den Letztverbraucher über die WAN-Schnittstelle (informativ)	

Tabelle 95: Tarifierungs-Anwendungsfälle

Im Kapitel 4.4.2 wird der allgemeine Testablauf für den Test eines TAF beschrieben. Besonderheiten, die bei den einzelnen TAF auftreten können und beachtet werden müssen, werden anschließend in den Kapiteln 4.4.3 bis 4.4.12 näher betrachtet.

Um das korrekte Verhalten der TAF 1 bis 10 zu testen, werden Positivtestfallketten erstellt. Die Testschritte einer Testfallkette bestehen aus Positivtestfällen aus den in Abbildung 14 aufgeführten Anwendungsfällen und ggf. aus neu zu beschreibenden Testschritten, wenn sich gewisse Abläufe nicht über die Positivtestfälle der in Abbildung 14 aufgeführten Anwendungsfälle abbilden lassen. Auf Negativtestfälle kann verzichtet werden, da die möglichen auftretenden Fehlersituationen in den Tests der Anwendungsfälle für WAN, HAN und LMN behandelt werden.

4.4.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	A	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	A	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	ja	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	nein	-
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	A	-
2	bekannte Sicherheitsrisiken und Angriffsszenarien	Auswahl (ja oder nein)	nein	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	B	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 96: Bewertungskriterien für Schnittstellen-übergreifend: Anwendungsfälle Tarifierung

4.4.2 Allgemeine Beschreibung zum Testablauf

Ein TAF kann als Abfolge von Anwendungsfällen der WAN-, HAN- und LMN-Schnittstelle abgebildet werden. Beachtet werden muss, dass die Abfolge der entsprechenden Anwendungsfälle in zeitlich korrekter Reihenfolge erfolgt. Die Repräsentation eines TAF durch Anwendungsfälle der WAN-, HAN- und LMN-Schnittstelle ist nachfolgend in Abbildung 14 dargestellt.

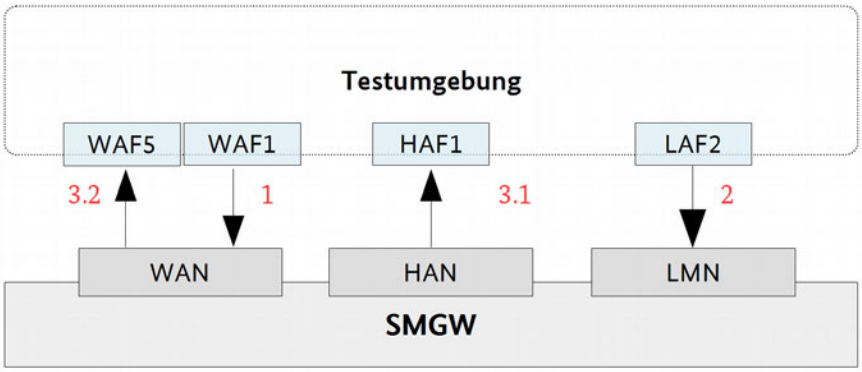

Abbildung 14: Repräsentation eines TAF durch Anwendungsfälle der WAN-, HAN- und LMN-Schnittstellen

Die Testumgebung muss hier die Rollen SMGW Administrator, EMT und Letztverbraucher zur Verfügung stellen.

Der Ablauf aller Positivtestfallketten gestaltet sich wie folgt:

- Der SMGW Administrator bringt mit Hilfe von Positivtestfällen des WAF1 verschiedene Geräte, Profile, Letztverbraucher und Schlüssel/Zertifikate in das SMGW ein und ordnet sie entsprechend zu (1). Mit verschiedenen Konstellationen der Parameter je Tarifart in den Auswertungsprofilen können so die internen Messwertverarbeitungsvorgänge implizit getestet werden.
- Die Zähler senden die für den jeweiligen TAF benötigten Messwerte an das SMGW, dies erfolgt mit Hilfe von Positivtestfällen des LAF2 (2).
- Das SMGW muss die Messwerte anhand des entsprechenden Regelwerks verarbeiten.
- Um zu testen, dass die Verarbeitung korrekt erfolgte, werden mit Hilfe von Positivtestfällen des HAF1 und des WAF5 die Werte vom SMGW abgefragt (3.1 und 3.2) und mit den in dem jeweiligen TAF beschriebenen Werten (siehe Kapitel 4.4.3 bis 4.4.12) verglichen.

In den Positivtestfallketten wird getestet, dass das SMGW die vom Zähler gelieferten Werte anhand des Regelwerks korrekt verarbeitet bzw. tarifiert , dann korrekt an die autorisierten Stellen weiterleitet und für den Letztverbraucher anforderungskonform an der HAN-Schnittstelle bereitstellt . Da das SMGW im Blackbox-Verfahren getestet wird, kann die Prüfung nur implizit erfolgen.

4.4.3 TAF1: Datensparsame Tarife (nach § 40 (5) EnWG)

Datensparsame Tarife sollen verhindern, dass das Verbrauchsverhalten der Letztverbraucher ausgewertet werden kann. Um dies zu erreichen, überträgt das SMGW von einem oder mehreren Zählern des Letztverbrauchers jeweils nur einen Zählerstand pro Abrechnungszeitraum an autorisierte externe Marktteilnehmer. Der Abrechnungszeitraum darf dabei nicht kleiner als ein Monat sein.

Die Auslieferung der Daten erfolgt zu dem im Regelwerk hinterlegten Versandzeitpunkt. Weiterhin muss das SMGW die zu versendenden Daten vor der Inhaltsdatenverschlüsselung mit einer zusätzlichen Signatur versehen.

Folgende Parameter müssen für das Regelwerk im Auswertungsprofil hinterlegt werden:

- Geräte-IDs der Zähler
- OBIS-Kennzahl der zu verwendenden Messgröße je Zähler
- Zählpunktbezeichnung
- Abrechnungszeitraum

- Letztverbraucherkennung
- Zugriffsberechtigungen
- Versandzeitpunkte
- Gültigkeitszeitraum

In der folgenden Tabelle sind Beispiel-Messwertsätze für die Auslieferung an einen EMT dargestellt:

Zeitstempel	Zählerstand Zähler 1	Zählerstand Zähler 2	Messwertsatz
01.01.2014 00:00:00	100 kWh	50 kWh	150 kWh
01.02.2014 00:00:00	180 kWh	110 kWh	290 kWh
01.03.2014 00:00:00	270 kWh	170 kWh	440 kWh

Tabelle 97: Beispiel für Messwertsätze, die an einen EMT geliefert werden

In der folgenden Tabelle wird dargestellt, welche Werte für den Letztverbraucher (LV) bereitgestellt und welche Werte zum jeweiligen Versandzeitpunkt an den externen Marktteilnehmer übermittelt werden:

Rolle	bereitzustellende bzw. zu übermittelnde Werte
Letztverbraucher	alle Parameter des Regelwerks
	die aktuellen Zählerstände und deren Summe
	die Differenzbeträge zum Ende des letzten Abrechnungszeitraums (mind. 15-minutengenau für Strom und 60-minutengenau für Gas)
	die bereits versendeten Zählerstände
	die Summe der bereits versendeten Zählerstände zum Ende jedes Abrechnungszeitraums innerhalb des letzten Jahres
	die Summe der bereits versendeten Zählerstände des jeweiligen Abrechnungszeitraums in den vergangenen 3 Jahren (Jahreswerte)
	die Messwertliste
Externer Marktteilnehmer	Summe der Zählerstände am Ende des jeweiligen Abrechnungszeitraums

Tabelle 98: für den LV bereitzustellende bzw. an den EMT zu übermittelnde Werte

4.4.4 TAF2: Zeitvariable Tarife (nach § 40 (5) EnWG)

Zeitvariable Tarife erlauben es dem Lieferanten, dem Letztverbraucher für unterschiedliche Zeiträume unterschiedliche Preise in Rechnung zu stellen. Dafür werden im Regelwerk unterschiedliche Tarifstufen mit Tarifumschaltzeitpunkten definiert. Zu jedem Zeitpunkt darf nur eine Tarifstufe aktiv sein und für jede Tarifstufe kumuliert das SMGW die Energiemenge, die in dieser Stufe angefallen ist.

Die Auslieferung der Daten erfolgt zu dem im Regelwerk hinterlegten Versandzeitpunkt. Weiterhin muss das SMGW die zu versendenden Daten vor der Inhaltsdatenverschlüsselung mit einer zusätzlichen Signatur versehen.

Folgende Parameter müssen für das Regelwerk im Auswertungsprofil hinterlegt werden:

- Geräte-IDs der Zähler
- OBIS-Kennzahl der zu verwendenden Messgröße je Zähler
- Zählpunktbezeichnung
- Definition der Tarifstufen

- Tarifumschaltzeitpunkte
- Abrechnungszeitraum
- Letztverbraucherkennung
- Zugriffsberechtigungen
- Versandzeitpunkte
- Gültigkeitszeitraum

In der folgenden Tabelle sind Beispiel-Messwertsätze für die Auslieferung an einen EMT dargestellt:

Tarifumschalt-zeitpunkt	Tarifstufe	Zählerstand Zähler 1	Zählerstand Zähler 2	Messwertsatz Tarifstufe 1	Messwertsatz Tarifstufe 2
01.01.2014 06:00:00	2	10	50	0	60
01.01.2014 22:00:00	1	30	80	50	60
02.01.2014 06:00:00	2	60	100	50	110
02.01.2014 22:00:00	1	100	200	190	110

Tabelle 99: Beispiel für Messwertsätze, die an einen EMT geliefert werden

In der folgenden Tabelle wird dargestellt, welche Werte für den Letztverbraucher bereitgestellt und welche Werte zum jeweiligen Versandzeitpunkt an den externen Marktteilnehmer übermittelt werden:

Rolle	bereitzustellende bzw. zu übermittelnde Werte
Letztverbraucher	alle Parameter des Regelwerks
	die aktuellen Zählerstände und die kumulierte Energie je Tarifstufe
	die Differenzbeträge zum Ende des letzten Abrechnungszeitraums (mindestens 15-minutengenau für Strom und 60-minutengenau für Gas)
	die Zählerstände und Stände der Tarifstufen zum Ende eines jeden Abrechnungszeitraumes innerhalb des letzten Jahres
	die Messwertliste
	alle an externe Marktteilnehmer versendete Daten
Externer Marktteilnehmer	kumulierte Energiemenge zum Ende des Abrechnungszeitraums für jede Tarifstufe
	bei Bedarf Bereitstellung der Tarifwechselliste

Tabelle 100: für den LV bereitzustellende bzw. an den EMT zu übermittelnde Werte

4.4.5 TAF3: Lastvariable Tarife

Lastvariable Tarife erlauben es dem Lieferanten, dem Letztverbraucher auf Basis der anfallenden Last den Verbrauch mit unterschiedlichen Preisen in Rechnung zu stellen. Dafür werden im Regelwerk unterschiedliche Laststufen mit Lastschwellen definiert. Eine Laststufe ist aktiv, wenn sich der Leistungsmittelwert bzw. die Momentanleistung zwischen der oberen und unteren Lastschwelle der Laststufe befindet. Wird eine Lastschwelle über- bzw. unterschritten, wird die Laststufe entsprechend gewechselt und ein Eintrag in der Messwertliste angelegt.

Die Auslieferung der Daten erfolgt zu dem im Regelwerk hinterlegten Versandzeitpunkt. Weiterhin muss das SMGW die zu versendenden Daten vor der Inhaltsdatenverschlüsselung mit einer zusätzlichen Signatur versehen.

Folgende Parameter müssen für das Regelwerk im Auswertungsprofil hinterlegt werden:

- Geräte-IDs der Zähler
- OBIS-Kennzahl der zu verwendenden Messgröße für die Energiemenge
- OBIS-Kennzahl der zu verwendenden Messgröße für die aktuelle Leistung
- Zählpunktbezeichnung
- Definition der Laststufen
- Registrierperiode
- Abrechnungszeitraum
- Letztverbraucherkennung
- Zugriffsberechtigungen
- Versandzeitpunkte
- Gültigkeitszeitraum

In der folgenden Tabelle sind Beispiel-Messwertsätze für die Auslieferung an einen EMT dargestellt, die Messwertliste wird anhand des Leitungsmittelwertes erzeugt:

Zeitstempel	Laststufe	Zählerstand	Leistungsmittelwert	Messwertsatz Laststufe 1	Messwertsatz Laststufe 2
01.01.2014 08:00:00	2	5 kWh	10 kW	5 kWh	0 kWh
01.02.2014 08:30:00	1	10 kWh	8 kW	5 kWh	5 kWh
01.03.2014 12:30:00	2	42 kWh	14 kW	37 kWh	5 kWh

Tabelle 101: Beispiel für Messwertsätze, die an einen EMT geliefert werden

In der folgenden Tabelle sind Beispiel-Messwertsätze für die Auslieferung an einen EMT dargestellt, die Messwertliste wird anhand der Momentanleistung erzeugt:

Zeitstempel	Laststufe	Zählerstand	Momentanleistung	Messwertsatz Laststufe 1	Messwertsatz Laststufe 2
01.01.2014 08:00:00	2	5 kWh	8 kW	5 kWh	0 kWh
01.02.2014 08:15:00	1	7 kWh	4 kW	5 kWh	2 kWh
01.03.2014 08:30:00	2	8 kWh	9 kW	6 kWh	2 kWh

Tabelle 102: Beispiel für Messwertsätze, die an einen EMT geliefert werden

In der folgenden Tabelle wird dargestellt, welche Werte für den Letztverbraucher bereitgestellt und welche Werte zum jeweiligen Versandzeitpunkt an den externen Marktteilnehmer übermittelt werden:

Rolle	bereitzustellende bzw. zu übermittelnde Werte
Letztverbraucher	alle Parameter des Regelwerks
	die aktuellen Zählerstände und die kumulierte Energie je Laststufe
	die Differenzbeträge zum Ende des letzten Abrechnungszeitraums (mind. 15-minutengenau für Strom und 60-minutengenau für Gas)
	die Momentanleistung (mindestens 15-minutengenau für Strom und 60-minutengenau für Gas)
	die Zählerstände und Stände der Tarifstufen zum Ende eines jeden Abrechnungszeitraumes innerhalb des letzten Jahres
	die Messwertliste
	alle an externe Marktteilnehmer versendete Daten
Externer Marktteilnehmer	kumulierte Energiemenge zum Ende des Abrechnungszeitraums für jede Laststufe
	bei Bedarf Bereitstellung der Tarifwechselliste

Tabelle 103: Tabelle 9: für den LV bereitzustellende bzw. an den EMT zu übermittelnde Werte

4.4.6 TAF4: Verbrauchsvariable Tarife

Verbrauchsvariable Tarife erlauben es, ein Mengenkontingent (z. B. 300 kWh) an zu verbrauchender Energiemenge in Verbrauchsstufen (z. B. Stufe 1: 50 kWh, Stufe 2: 200 kWh, Stufe 3: 400 kWh) einzuteilen. Ist ein Kontingent aufgebraucht (z. B. Stufe 1 mit 50 kWh), wird die nächst höhere Verbrauchsstufe (Stufe 2 mit 200 kWh) aktiviert. In der Messwertliste wird immer zum Beginn/Ende einer Abrechnungsperiode und beim Wechsel der Verbrauchsstufe ein Eintrag erzeugt. Weiterhin dürfen nur Zähler verwendet werden, die nur den Verbrauch oder nur die Einspeisung messen. Wird ein anderer Zähler verwendet, erzeugt das SMGW im eich-technischen Log einen Eintrag.

Die Auslieferung der Daten erfolgt zu dem im Regelwerk hinterlegten Versandzeitpunkt. Weiterhin muss das SMGW die zu versendenden Daten vor der Inhaltsdatenverschlüsselung mit einer zusätzlichen Signatur versehen.

Folgende Parameter müssen für das Regelwerk im Auswertungsprofil hinterlegt werden:

- Geräte-IDs der Zähler
- OBIS-Kennzahl der zu verwendenden Messgröße je Zähler
- Zählpunktbezeichnung
- Registrierperiode
- Definition der Verbrauchsstufen
- Abrechnungszeitraum
- Letztverbraucherkennung
- Zugriffsberechtigungen
- Versandzeitpunkte
- Gültigkeitszeitraum

In der folgenden Tabelle sind Beispiel-Messwertsätze für die Auslieferung an einen EMT dargestellt:

Zeitstempel	Verbrauchsstufe	Zählerstand Zähler	Messwertsatz
01.01.2014 00:00:00	1 (Start)	0 kWh	0 kWh
10.01.2014 13:00:00	2	50 kWh	50 kWh
25.01.2014 08:00:00	3	200 kWh	200 kWh
01.02.2014 00:00:00	1 (Start)	230 kWh	230 kWh

Tabelle 104: Beispiel für Messwertsätze, die an einen EMT geliefert werden

2577 In der folgenden Tabelle wird dargestellt, welche Werte für den Letztverbraucher bereitgestellt und welche
2578 Werte zum jeweiligen Versandzeitpunkt an den externen Marktteilnehmer übermittelt werden:

Rolle	bereitzustellende bzw. zu übermittelnde Werte
Letztverbraucher	alle Parameter des Regelwerks
	die aktuellen Zählerstände und die Stände der Verbrauchsstufen
	die Differenzbeträge zum Ende des letzten Abrechnungszeitraums (mind. 15-minutengenau für Strom und 60-minutengenau für Gas)
	die aktuellen verbleibenden Kontingente der Tarifstufen
	die Zählerstände und Stände der Verbrauchsstufen zum Ende jedes Abrechnungszeitraums innerhalb des letzten Jahres
	die Messwertliste
	alle an externe Marktteilnehmer versendete Daten
Externer Marktteilnehmer	Summe der Zählerstände zum Ende des Abrechnungszeitraums
	Messwertliste ohne Zählerstände

Tabelle 105: für den LV bereitzustellende bzw. an den EMT zu übermittelnde Werte

2579 4.4.7 TAF5: Ereignisvariable Tarife

2580 Ereignisvariable Tarife enthalten mehrere Tarifstufen, zwischen denen auf Grund eines auftretenden
2581 Ereignisses gewechselt wird. Jeder Tarifstufe wird dazu mindestens ein Ereignis zugeordnet. Die Ereignisse
2582 können ausgelöst werden durch:

2583 • ein SMGW-internes Ereignis (kann vom SMGW unterstützt werden)

2584 • einen externen Markteilnehmer (muss vom SMGW unterstützt werden)

2585 • ein CLS (kann vom SMGW unterstützt werden)

2586 Es muss vom SMGW geprüft werden, ob eine Tarifumschaltung durchgeführt werden darf oder nicht. Dazu
2587 werden bei der Konfiguration der Ereignisse und in der Tarifumschaltanweisung Bedingungen hinterlegt.
2588 Stimmen die Bedingungen nicht überein, wird das gesendete Ereignis verworfen und der SMGW
2589 Administrator wird informiert (siehe 4.1.3).

2590 Es kann immer nur eine Tarifstufe aktiv sein und das SMGW kumuliert für jede Tarifstufe die verbrauchte
2591 Energiemenge. Weiterhin wird bei jedem Tarifstufenwechsel ein Eintrag in der Messwertliste angelegt.

2592 Die Auslieferung der Daten erfolgt zu dem im Regelwerk hinterlegten Versandzeitpunkt. Weiterhin muss
2593 das SMGW die zu versendenden Daten vor der Inhaltsdatenverschlüsselung mit einer zusätzlichen Signatur
2594 versehen.

2595 Folgende Parameter müssen für das Regelwerk im Auswertungsprofil hinterlegt werden:

2596 • Geräte-IDs der Zähler

- OBIS-Kennzahl der zu verwendenden Messgröße je Zähler
- Zählpunktbezeichnung
- Definition der Tarifstufen
- Konfiguration der Ereignisse für Tarifstufen
- Abrechnungszeitraum
- Letztverbraucherkennung
- Zugriffsberechtigungen
- Versandzeitpunkte
- Gültigkeitszeitraum

In der folgenden Tabelle sind Beispiel-Messwertsätze für die Auslieferung an einen EMT dargestellt:

Zeitstempel	Ereignis	Tarifstufe	Zählerstand Zähler	Messwertsatz Tarifstufe 1	Messwertsatz Tarifstufe 2
01.01.2014 00:00:00	Ende/Beginn	1	0 kWh	0 kWh	0 kWh
15.01.2014 00:00:00	Firmen-jubiläum	2	110 kWh	110 kWh	0 kWh
19.01.2014 00:00:00	Ende Firmen-jubiläum	1	200 kWh	110 kWh	90 kWh
01.02.2014 00:00:00	Ende/Beginn	1	250 kWh	160 kWh	90 kWh

Tabelle 106: Beispiel für Messwertsätze, die an einen EMT geliefert werden

In der folgenden Tabelle wird dargestellt, welche Werte für den Letztverbraucher bereitgestellt und welche Werte zum jeweiligen Versandzeitpunkt an den externen Marktteilnehmer übermittelt werden:

Rolle	bereitzustellende bzw. zu übermittelnde Werte
Letztverbraucher	alle Parameter des Regelwerks
	die aktuellen Zählerstände und die kumulierte Energiemenge je Tarifstufe
	die Differenzbeträge zum Ende des letzten Abrechnungszeitraums (mind. 15-minutengenau für Strom und 60-minutengenau für Gas)
	die Zählerstände und Stände der Tarifstufen zum Ende eines jeden Abrechnungszeitraumes innerhalb des letzten Jahres
	die Messwertliste (Tarifwechselliste mit Zählerständen und den zugehörigen abgeleiteten Registern)
	alle an externe Marktteilnehmer versendete Daten
Externer Marktteilnehmer	kumulierte Zählerstände für jede Tarifstufe
	bei Bedarf Bereitstellung der Tarifwechselliste ohne Zählerstände

Tabelle 107: für den LV bereitzustellende bzw. an den EMT zu übermittelnde Werte

4.4.8 TAF6: Abruf von Messwerten im Bedarfsfall

Für den Bedarfsfall muss das SMGW für alle Zähler und abgeleitete Register die Messwerte taggenau vorhalten. Da die Messwerte rückwirkend abrufbar sein sollen, reicht es hier aus, die Ergebnisse anderer Tarifierungstestfallketten auch unter diesem Gesichtspunkt zu prüfen. Auch das Vorhalten der täglichen Messdaten je Zähler und abgeleitetem Register für 6 Wochen soll überprüft werden.

Folgende Parameter müssen für das Regelwerk im Auswertungsprofil hinterlegt werden:

- Geräte-IDs der Zähler
- OBIS-Kennzahl der zu verwendenden Messgröße je Zähler
- Zählpunktbezeichnung
- Beginn des abrechnungstechnischen Kalendertags
- Letztverbraucherkennung

Zeitstempel	Zählerstand Zähler 1	Zählerstand Zähler 2	Register 1	Register2
05.09.2014 06:00:00	100 kWh	90 kWh	250 kWh	220 kWh

Tabelle 108: Beispiel für Messwertsätze, die an einen EMT geliefert werden

In der folgenden Tabelle wird dargestellt, welche Werte für den Letztverbraucher bereitgestellt und welche Werte zum jeweiligen Versandzeitpunkt an den externen Marktteilnehmer übermittelt werden:

Rolle	bereitzustellende bzw. zu übermittelnde Werte
Letztverbraucher	Alle Parameter des Regelwerks
	Tagesgenaue Stände aller ihm zugeordneter Zähler und abgeleiteten Registern der SMGW
	Liste der Zeitpunkte, zu denen SMGW Administrator Messwerte abgerufen hat
Externer Marktteilnehmer	Zählerstände und Stände der abgeleiteten Register für den angefragten Stichtag (innerhalb der letzten 6 Wochen)

Tabelle 109: für den LV bereitzustellende bzw. an den EMT zu übermittelnde Werte

4.4.9 TAF7: Zählerstandsgangmessung

In diesem Anwendungsfall werden im Takt der Registrierperiode die konkreten Lastwerte eines Zählers erfasst, in einer Messwertliste abgespeichert und zu definierten Versandzeitpunkten an den berechtigten externen Marktteilnehmer

Folgende Parameter müssen für das Regelwerk im Auswertungsprofil hinterlegt werden:

- Geräte-IDs der Zähler
- OBIS-Kennzahl der zu verwendenden Messgröße je Zähler
- Zählpunktbezeichnung
- Registrierperiode
- Abrechnungszeitraum
- Letztverbraucherkennung

- Zugriffsberechtigungen
- Versandzeitpunkte
- Gültigkeitszeitraum

Zeitstempel	Zähler 1	Zähler 2	Zähler 3
01.01.2014 06:15:00	15 kWh	130 kWh	1.200 kWh
01.01.2014 06:30:00	15 kWh	130 kWh	1.2000 kWh
01.01.2014 06:45:00	35 kWh	150 kWh	1.205 kWh
01.01.2014 07:00:00	95 kWh	150 kWh	1.230 kWh
...	...	...	...
31.01.2014 23:30:00	390 kWh	755 kWh	1.750 kWh
31.01.2014 23:45:00	390 kWh	755 kWh	1.780 kWh

Tabelle 110: Beispiel für Zählerstandsgänge, die an einen EMT geliefert werden

In der folgenden Tabelle wird dargestellt, welche Werte für den Letztverbraucher bereitgestellt und welche Werte zum jeweiligen Versandzeitpunkt an den externen Marktteilnehmer übermittelt werden:

Rolle	bereitzustellende bzw. zu übermittelnde Werte
Letztverbraucher	Alle Parameter des Regelwerks
	Aktuelle Zählerstände aller ihm zugeordneter Zähler und abgeleiteten Registern der SMGW
	Liste der Zeitpunkte, zu denen SMGW-Admin Messwerte abgerufen hat
Externer Marktteilnehmer	Aktuelle Zählerstände aller ihm zugeordneter Zähler und abgeleiteten Registern der SMGW

Tabelle 111: für den LV bereitzustellende bzw. an den EMT zu übermittelnde Werte

4.4.10 TAF8: Erfassung von Extremwerten für Leistung

Zur Erfassung von Minimal- und Maximalleistungswerten erfasst das SMGW in regelmäßigen Abständen (Registrierperiode) aktuelle Zählerstände und errechnet für diese Perioden den Leistungsmittelwert. Die höchsten und niedrigsten Werte im Abrechnungszeitraum werden dann zu definierten Versandzeitpunkten an den autorisierten externen Marktteilnehmer übermittelt.

Folgende Parameter müssen für das Regelwerk im Auswertungsprofil hinterlegt werden:

- Geräte-IDs der Zähler
- OBIS-Kennzahl der zu verwendenden Messgröße je Zähler
- Zählpunktbezeichnung
- Registrierperiode
- Anzahl Minimalwerte n
- Anzahl Maximalwert m
- Abrechnungszeitraum
- Letztverbraucherkennung
- Zugriffsberechtigungen

- Versandzeitpunkte

Zeitstempel	Minimum Zähler 1
23.01.2014 02:00:00	0 kWh
11.01.2014 02:30:00	0 kWh
16.01.2014 03:30:00	2 kWh

Tabelle 112: Beispiel für einen Minimummesswertsatz, der an einen EMT geliefert wird (n=3)

Zeitstempel	Maximum Zähler 1
23.01.2014 17:45:00	66 kWh
11.01.2014 19:30:00	63 kWh

Tabelle 113: Beispiel für einen Maximummesswertsatz, der an einen EMT geliefert wird (m=2)

In der folgenden Tabelle wird dargestellt, welche Werte für den Letztverbraucher bereitgestellt und welche Werte zum jeweiligen Versandzeitpunkt an den externen Marktteilnehmer übermittelt werden:

Rolle	bereitzustellende bzw. zu übermittelnde Werte
Letztverbraucher	Alle Parameter des Regelwerks
	n niedrigste Leistungsmittelwerte eines Zählers im Abrechnungszeitraum
	m höchste Leistungsmittelwerte eines Zählers im Abrechnungszeitraum
	Liste aller Messwerte
	Liste der Zeitpunkte, zu den SMGW-Admin Messwerte abgerufen hat
Externer Marktteilnehmer	n niedrigste Leistungsmittelwerte eines Zählers im Abrechnungszeitraum
	m höchste Leistungsmittelwerte eines Zählers im Abrechnungszeitraum

Tabelle 114: für den LV bereitzustellende bzw. an den EMT zu übermittelnde Werte

4.4.11 TAF9: Abruf der Ist-Einspeisung einer Erzeugungsanlage

Der berechtigte externe Marktteilnehmer darf zu beliebigen Zeitpunkten die Ist-Einspeisungsleistung einer Erzeugungsanlage abfragen. Der Leistungswert wird ohne Messwertliste direkt an den externen Marktteilnehmer versandt.

Folgende Parameter müssen für das Regelwerk im Auswertungsprofil hinterlegt werden:

- Geräte-IDs der Zähler
- OBIS-Kennzahl der zu verwendenden Messgröße je Zähler
- Zählpunktbezeichnung
- Abrechnungszeitraum
- Letztverbraucherkennung
- Zugriffsberechtigungen
- Versandzeitpunkte
- Gültigkeitszeitraum

In der folgenden Tabelle wird dargestellt, welche Werte für den Letztverbraucher bereitgestellt und welche Werte zum jeweiligen Versandzeitpunkt an den externen Marktteilnehmer übermittelt werden:

Rolle	bereitzustellende bzw. zu übermittelnde Werte
Letztverbraucher	Alle Parameter des Regelwerks
	Aktuelle Ist-Einspeisungsleistung seiner Erzeugungsanlage
	Alle Daten, die an externe Marktteilnehmer verschickt wurden
Externer Marktteilnehmer	Aktuelle Ist-Einspeisungsleistung der Erzeugungsanlage

Tabelle 115: für den LV bereitzustellende bzw. an den EMT zu übermittelnde Werte

4.4.12 TAF10: Abruf von Netzzustandsdaten

Beim Eintritt definierter Ereignis sollen bestimmte Zählerwerte oder Messgrößen zum Netzzustand an berechtigte externe Marktteilnehmer gesendet werden.

Abzuprüfende Ereignisse sind mindestens:

- Auslösung durch SMGW Administrator
- Ein Messwert (z. B. Lastflüsse, Phasenwinkel, Spannung, Frequenz und Stromfluss) über- oder unterschreitet einen Schwellwert
- Durch konkrete Statusinformation direkt von den Zählern

Folgende Parameter müssen für das Regelwerk im Auswertungsprofil hinterlegt werden:

- Geräte-IDs der Zähler
- OBIS-Kennzahl der zu verwendenden Messgröße je Zähler
- Zählpunktbezeichnung
- Statusinformationen (optional)
- Letztverbraucherkennung
- Zugriffsberechtigungen
- Ereignisse
- Pseudonym

In der folgenden Tabelle wird dargestellt, welche Werte für den Letztverbraucher bereitgestellt und welche Werte zum jeweiligen Versandzeitpunkt an den externen Marktteilnehmer übermittelt werden:

Rolle	bereitzustellende bzw. zu übermittelnde Werte
Letztverbraucher	Alle Parameter des Regelwerks
Externer Marktteilnehmer	Liste von ausgewählten Messwerten der Netzzustandsdaten

Tabelle 116: für den LV bereitzustellende bzw. an den EMT zu übermittelnde Werte

4.4.13 Testeingangskriterien, Abhängigkeiten

Die Protokoll- und Anwendungsfalltests der LMN-, HAN- und WAN-Schnittstellen sowie die Tests des SecMod müssen erfolgreich durchgeführt worden sein.

4.4.14 Testdaten

Für die Tests zur Tarifierung müssen folgende Testdaten vorhanden sein:

- der SMGW Administrator muss mit einem gültigen Zertifikat und seiner Kommunikationsadresse im SMGW eingerichtet sein
- mehrere Letztverbraucher müssen im SMGW vorhanden sein (man könnte z. B. die in der Mandatenverwaltung angelegten Letztverbraucher nutzen)
- mehrere Zähler müssen im SMGW vorhanden sein (man könnte z. B. die in der Geräteverwaltung und Profilverwaltung angelegten Zähler nutzen)
- es müssen verschiedene Messwerte für verschiedene Zähler für die Auslieferung vorhanden sein
- mehrere externe Marktteilnehmer müssen im SMGW vorhanden sein (man könnte z. B. die in der Profilverwaltung angelegten Kommunikationsprofile nutzen)
- es muss das TAF-spezifische Auswertungsprofil mit verschiedenen Regelwerksparametern vorhanden sein (man könnte z. B. die in der Profilverwaltung angelegten Auswertungsprofile nutzen)

4.4.15 Hinweise zu möglichen Testwerkzeugen (informativ)

Keine.

4.5 Weitere Testelemente und Testfälle

In diesem Kapitel werden weitere, aus funktionalen Anforderungen ohne direkten Schnittstellen- oder Anwendungsfallbezug abgeleitete Testfälle beschrieben.

4.5.1 Versiegelung

Es sind Testfälle durchzuführen, die den geforderten lokalen Zugriffsschutz des Testobjektes nachweisen. Der Schutz ist durch geeignete Siegel zu realisieren, die eine physische Manipulation des Testobjektes erkennbar machen.

Nicht zu überprüfen sind Anforderungen, die lediglich in konkreten Einbausituation Bedeutung erhalten (montage-, nicht bauartbedingte Umstände).

ID	**Anforderung (abstrakt)**	**Konkretisierung [BSI TR-03109-1]**	**Zusätzliche Referenz(en)**
	Übergreifende Anforderung	*Anforderung*	*Anforderungsquelle*
__.SON.01	Das SMGW MUSS sich gegen Angriffe schützen, die einen lokalen Zugriff auf das SMGW voraussetzen.	-	[BSI TR-03109-1] [GW_PP]
__.SON.01.01	__.SON.01	Das SMGW MUSS durch Verwendung eines geeigneten Siegels physikalische Manipulationen erkennbar machen.	-
__.SON.01.02	__.SON.01	Es DARF NICHT möglich sein, das SMGW-Gehäuse zu öffnen, ohne das Siegel erkennbar zu brechen.	-

ID	Anforderung (abstrakt)	Konkretisierung [BSI TR-03109-1]	Zusätzliche Referenz(en)
	Übergreifende Anforderung	*Anforderung*	*Anforderungsquelle*
__.SON.01.03	__.SON.01	Das Siegel MUSS auf geeigneten Siegelflächen angebracht werden, so dass es im normalen Betrieb nicht durch Abnutzung gebrochen wird.	-
__.SON.01.04	__.SON.01	Ist das Siegel nach Einbau des SMGW nicht mehr sichtbar, MUSS die Unversehrtheit durch vor Montage geprüft und durch zusätzliche Plombierung einer über dem SMGW liegenden Abdeckung gesichert werden. Hinweis: Diese Anforderung wird nicht im Rahmen hier spezifizierter Tests nachgewiesen, sondern kann erst bei tatsächlichem Einbau realisiert werden.	-
__.SON.01.05	__.SON.01	Das Gehäuse MUSS geeignet sein, unbemerkte Manipulationen ohne Bruch des Siegels zu verhindern	-
__.SON.01.05.01	SON.01.05	Mit Ausnahme der notwendigen Schnittstellenzugänge und Lüftungsöffnungen MUSS das Gehäuse geschlossen sein.	-
__.SON.01.05.02	SON.01.05	Vorhandene Öffnungen DÜRFEN KEINE Manipulationen zulassen.	-
__.SON.01.06	__.SON.01	Siegel MÜSSEN in der gesicherten Produktionsumgebung des Herstellers angebracht werden.	-
__.SON.01.07	__.SON.01	Ein SMGW SOLL das Öffnen des Gehäuses detektieren und darauf reagieren können.	-
__.SON.01.07.01	__.SON.01.07	Im Falle der Gehäuseöffnung SOLL der SMGW Administrator kontaktiert werden.	-

ID	Anforderung (abstrakt)	Konkretisierung [BSI TR-03109-1]	Zusätzliche Referenz(en)
	Übergreifende Anforderung	*Anforderung*	*Anforderungsquelle*
__.SON.01.07.02	__.SON.01.07	Das Ereignis „Gehäuse geöffnet“ SOLL im Eichtechnischen Log und im System-Log protokolliert werden.	-

Tabelle 117: Anforderungen Versiegelung

2733 4.5.1.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	nicht relevant	Anforderungen beziehen sich nicht auf Interoperabilität
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	B	Bei Realisierung der Detektierungsoptionen wird B angenommen, ansonsten kann C angesetzt werden
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	ja	in Bezug auf die Detektierung von Gehäuseöffnungen / Aufzeichnung in Logdateien
2	Implementierung in Hardware	Auswahl (ja oder nein)	ja	Ausnahme: Detektierungsoptionen
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	C	-
	Informativ: bekannte Sicherheitsrisiken und Angriffsszenarien	Auswahl (ja oder nein)	ja	in Bezug auf Siegelbruch / -manipulation
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	hinsichtlich Gehäuseschutz: in Anlehnung an für Zähler etablierte Verfahren
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	A	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	Einbauspezifische Tests und Tests in Bezug auf die Siegelanbringung sind auszuschließen

Tabelle 118: Bewertungskriterien für Versiegelung

2734 4.5.1.2 Testeingangskriterien, Abhängigkeiten

2735 Die Anforderung, dass erforderliche Siegel in der gesicherten Produktionsumgebung des Herstellers
2736 angebracht werden, soll im Rahmen der CC-Evaluierung erfolgen.

Siegelzerstörende Prüfungen sollen am Ende der Testdurchführung vorgenommen werden. Die dahingehenden Tests sind fotografisch unter Angabe von Datum und Uhrzeit der Testdurchführung zu dokumentieren. Dazu gehört unbedingt auch der Zustand des Testobjektes vor der Durchführung von Tests, die Siegel zerstören können, um die Integrität des Testobjektes bis zu diesem Zeitpunkt nachweisen zu können.

Es kann unter Umständen erforderlich sein, dass für die Tests mehrere baugleiche SMGW notwendig sind.

Die übergebene Produktdokumentation MUSS eine Aussage darüber treffen, welche der nach [BSI TR-03109-1] optionalen Anforderungen realisiert wurden (Detektierung und Protokollierung).

4.5.1.3 Testdaten

Es sind keine Testdaten vorgegeben.

4.5.1.4 Testdurchführung

Nachfolgende Tabelle gibt eine Übersicht über die vorzusehenden Tests.

Anforderungs-referenz	Testfokus	Durchführung	Erwartetes Verhalten
__.SON.01 __.SON.01.01 __.SON.01.02 __.SON.01.03	Vorhandensein und Eignung von Siegeln	Sichtprüfung und manueller Test auf Entfernen sowie Zerstörung bei Öffnungsversuchen (manuelle Tests), formular- bzw. checklistengeführt und fotodokumentiert	• Siegel sind in ausreichendem Maß vorhanden • Siegel lassen sich nicht ohne sichtbare Spuren am Siegel entfernen und wieder aufbringen • Siegel werden bei Öffnung / Öffnungsversuch zerstört
__.SON.01 __.SON.01.05 __.SON.01.05.01 __.SON.01.05.02	Vorhandensein von Öffnungen	Sichtprüfung, formular- bzw. checklistengeführt und fotodokumentiert	Es sind keine Gehäuseöffnungen vorhanden, die mit handelsüblichem Werkzeug Manipulationen im SMGW ohne Öffnen des Gehäuses ermöglichen.
__.SON.01 __.SON.01.07 __.SON.01.07.01 __.SON.01.07.02	Detektierung und Protokollierung von Gehäuseöffnungen	Kombinierter manueller Test mit Tests integriert in die Testumgebung; kombinierbar mit Öffnungsversuch	Sind die SOLL-Anforderungen realisiert, wird bei Öffnen • eine qualifizierte Nachricht an den SMGW Administrator versandt und • insofern implementiert, werden Log-Einträge erzeugt

Tabelle 119: Testdurchführung

Wurde für das SMGW eine modulare Bauweise (z. B. für optionale oder austauschbare Kommunikationseinheiten wie UMTS oder W-LAN) gewählt, muss die Einbauanleitung dahingehend überprüft werden, dass eine am Einbauort erforderliche Zugriffssicherung vorgeschrieben ist. Eine modulare Bauweise ist auch dahingehend zu bewerten, ob sich zusätzliche Angriffspunkte ergeben, welche die Anforderungen der [BSI TR-03109-1] betreffen.

4.5.1.5 Hinweise zu möglichen Testwerkzeugen (informativ)

Für die Durchführung der Tests zur Benachrichtigung des SMGW Administrators ist auf den Testaufbau wie für Tests gemäß Kapitel 4.1.3 (WAF3: Alarmierung und Benachrichtigung) zurückzugreifen.

Für die Durchführung der Tests hinsichtlich der Erzeugung von Log-Einträgen ist auf den Testaufbau wie für Tests gemäß Kapitel 4.1.1.8 (SMGW Monitoring)zurückzugreifen.

4.5.2 Einbau des Sicherheitsmoduls

Der herstellerseitig zu führende Nachweis über den anforderungskonformen Einbau des Sicherheitsmoduls ist durch einen Dokumentationstest zu bestätigen. Dieser prüft, ob die vorgeschriebenen Bescheinigungen in gültiger Fassung vorliegen und sich auf das Testobjekt beziehen.

ID	**Anforderung (abstrakt)**	**Konkretisierung [BSI TR-03109-1]**	**Zusätzliche Referenz(en)**
	Übergreifende Anforderung	*Anforderung*	*Anforderungsquelle*
__.SON.02	Die zur gegenseitigen Authentisierung zwischen SMGW und SecMod benötigte PIN MUSS geeignet geschützt sein.	-	[BSI TR-03109-1]
__.SON.02.01	__.SON.02	Der Schutzmechanismus MUSS von einer CC-Prüfstelle begutachtet und dem BSI in Form einer Herstellererklärung nachgewiesen worden sein.	[BSI TR-03109-3]

Tabelle 120: Anforderungen Einbau Sicherheitsmodul

4.5.2.1 Testelementbewertung

Bewertungs-ebene	Kriterium	Bewertungs-maßstab	Bewertungs-ergebnis	Erläuterung / Begründung
1	Interoperabilitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	nicht relevant	-
1	Funktionalitäts-vorgaben	Gewichtung (A ... C laut Tabelle 8)	C	-
2	TR-spezifische Anforderung	Auswahl (ja oder nein)	ja	-
2	Implementierung in Hardware	Auswahl (ja oder nein)	ja	aus Sicht der TS: Hardware ist hierbei das SMGW-Produkt als Ganzes
2	Konfigurations-möglichkeiten	Gewichtung (A ... C laut Tabelle 8)	nicht relevant	-
2	Testbarkeit mit bekannten Testarten	Auswahl (ja oder nein)	ja	-
3 (projekt-spezifisch)	Anforderungsstabilität	Gewichtung (A ... C laut Tabelle 8)	A	-
3 (projekt-spezifisch)	Testbarkeit mit festgelegten Testarten	Auswahl (ja oder nein)	ja	-

Tabelle 121: Bewertungskriterien für Einbau des Sicherheitsmoduls

4.5.2.2 Testeingangskriterien, Abhängigkeiten

Die Durchführung des Dokumententests setzt einen positiven Nachweis der durchgeführten CC-Evaluierung voraus

4.5.2.3 Testdaten

- Herstellererklärung

4.5.2.4 Testdurchführung

Nachfolgende Tabelle gibt eine Übersicht über die vorzusehenden Tests.

Anforderungs-referenz	Testfokus	Durchführung	Erwartetes Verhalten
__.SON.02 __.SON02.01	Dokumententest	• Bestätigung des Vorliegens des Nachweises • Bestätigung der korrekten Versionen (das nachgewiesene Verfahren ist auf das Testobjekt in aktueller Version (Bauart, Modell) anwendbar	Nachweis liegt vor und gilt für das Testobjekt.

Tabelle 122: Testdurchführung

4.5.2.5 Hinweise zu möglichen Testwerkzeugen (informativ)

Keine.

5 Testdrehbuch

Kapitel 5 hat informativen Charakter.

Dieses Kapitel enthält Hinweise zur Testablaufspezifikation, die sich aus den Abhängigkeiten der Testfälle zueinander durch Vor- und/oder Nachbedingungen ergeben und beachtet werden müssen (5.3).

Im Ergebnis der AP 2 und 3 erfolgt die vollständige Ermittlung der Abhängigkeiten (beispielhaft in 5.3 dargestellt) und es werden auch die Testsuiten näher erläutert werden (5.4).

Außerdem werden Hinweise zum Testablauf gegeben, die von einer testdurchführenden Stelle berücksichtigt werden können (5.5).

Die TS definiert über die in den Testfällen und -konfigurationen getroffenen Vorgaben (Vor- und Nachbedingungen) hinaus grundsätzlich keine Testabläufe.

5.1 Allgemeine Testreihenfolge

Die Reihenfolge der Testaktivitäten wird grob wie folgt anzulegen sein:

(0) Testvoraussetzungen und statische Tests (Prüfung der Herstellerdokumentation)

(1) Test der Technische Interoperabilität

(1.1) Test der Anbindung (Integration in Testumgebung)

(1.2) Test der Verbindung (Verfügbarkeit explizit geforderter Protokolle und Protokollanpassungen)

Subset: Protokoll-Einzeltests auf explizite Funktionsforderungen in gleichartiger Reihenfolge

(1.3) Test der syntaktischen Interoperabilität – Kommunikationsszenarien

(2) Semantische Interoperabilität: Anwendungsfälle (inkludiert Test der geforderten Funktionen)

(3) Sonstige Tests außerhalb der Testumgebung

Punkt (2) kann wesentliche Teile von Punkt (1.3) enthalten (vgl. gewählter Testansatz, Kapitel 5.2).

Punkt (1) kann auch als sog. Smoketest für die Tests zu Punkt (2) betrachtet werden.

5.2 Testansatz aus Testabdeckungsperspektive

Die Testspezifikation erreicht die für die Konformitätsbewertung als notwendig und technisch möglich angesehene Testabdeckung durch das Verfolgen einen Top-Down-Testansatzes bezogen auf das OSI-Schichtenmodell. Es soll eine möglichst vollständige Testabdeckung auf Anwendungsebene erreicht werden und gleichzeitig mit den expliziten Tests durch geeignete PCO-Setzung eine Testabdeckung für darunter liegende Schichten erzielt werden. Die Zahl der expliziten Testfälle auf einer OSI-Schicht nimmt dementsprechend von Schicht 7 zu Schicht 1 ab. Der Testablauf wird diesen Ansatz reflektieren.

5.3 Vorgaben für den Testablauf

Nachfolgend werden beispielhaft die sich aus den Abhängigkeiten der Anforderungen und Testbedingungen ergebenden Vorgaben an den Testablauf aufgeführt.

Tabelle 123 listet die zu beachtenden Abhängigkeiten von Testfällen exemplarisch auf. Es wird auf Testfallgruppen referenziert. Die Aufzählung der Spalte „#“ gibt keine weitere Reihenfolge vor.

#	Referenzpunkt (Kapitel)	Testfälle - (optional) Beschreibung der Abhängigkeit / Hinweis	Voraussetzung für Nachfolger (Kapitel)
1	2.3	Dokumententest: Testeingangskriterien validieren	3 und 4
2	3.2	Dokumententest und/oder Test auf implementierte Protokolle auf den OSI-Ebenen 1-4 an der WAN-Schnittstelle: verwendbare Implementierung vorhanden	4.1
3	3.2.1	Tests der TLS-Implementierung für die WAN-Schnittstelle sind erfolgreich	3.2.2, 3.2.7
4	...	Tests der HTTP-Implementierung für die WAN-Schnittstelle sind erfolgreich	...
5	...	Tests der COSEM-Webservices an der WAN-Schnittstelle sind erfolgreich	...
...	...	...	...

Tabelle 123: Beispielhafter Ausschnitt: Abhängigkeiten im Testablauf

Die Abhängigkeiten werden wie in Kapitel 2.4 beschrieben in der Spezifikation abgebildet.

5.4 Testsuite(n)

Dieses Kapitel (5.4) hat informativen Charakter.

Kapitel 2.4 definiert grundsätzlich genau eine Testsuite. Die TS wird diese Testsuite nach Möglichkeit so vorgeben, dass eine thematische und an der erwarteten Systemarchitektur orientierte Gliederung, Pflege und ggf. auch Separierung möglich wird. Dabei werden mindestens die folgenden Aspekte berücksichtigt:

- thematische Kapselung: Metering, Gesichtspunkte dazu sind
  - eichrechtliche Relevanz
  - stabile / fixierte Schnittstellen (vgl. übliche Dauer des Feldeinsatzes für einen Zähler)
  - erwartet: Implementierung der Datenhaltung und -aggregation von Zähler-gelieferten Daten erfolgt in einem (oder mehreren) dedizierten Software-Modulen / Firmwareteilen[47]
- thematische Kapselung: Gateway-Funktionen (Proxy-Funktionen)
- Quellen/Ersteller der Testspezifikation (bei Nutzung von Drittspezifikationen, z. B. VDE/FNN)

An dieser Stelle werden für die Testspezifikation Erläuterungen zu der (den) Testsuite(n) aufgenommen.

Die Testsuite(n) soll(en) stets so aufgebaut und in sich beschrieben sein, dass möglichst einfach Änderungen und Fortschreibungen an der Spezifikation möglich sind.

5.5 Hinweise zum Testablauf

Dieses Kapitel (5.5) hat informativen Charakter.

47 [BSI TR-03109-1] gibt hierzu aktuell keine hinreichende Architektur-Vorgabe; um die funktionalen und nicht-funktionalen Anforderungen zu erfüllen, wird jedoch eine solche Implementierung angenommen – diese ist auch erforderlich, um die Integrität bei Änderungen an anderen Stellen der Firmware für eichrechtlich relevante Bereiche sicher zu stellen.

Ein Ansatz für den zeitlichen Ablauf der Konformitätstests kann durch Zusammenfassung von Testfällen in Testszenarien in Anlehnung an das OSI-Schichtenmodell gewählt werden, wobei die unter 5.1 gegebenen Hinweise berücksichtigt werden sollten:

Testphase #	Inhalt	Hinweise
0	Dokumentationsprüfung	-
1	Protokolltests OSI-Schichten 1 - 4	-
2	Schlüsselaustausch	-
3	Kryptografische Vorgaben	-
4	Protokolltests OSI-Schichten 5 - 7	-
5	Identifizierung	-
6	Autorisierung	-
7	Anwendungsfälle	-
8	sonstige nicht-funktionale Anforderungen	-

Tabelle 124: Empfehlung zur Reihenfolge von Testphasen

2823 # Literatur- und Referenzverzeichnis

Literaturverzeichnis

BSI TR-03109: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-03109 (Version 1.0), 2013

BSI TR-03109-1: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-03109-1 "Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems" (Version 1.0), 2013

BSI TR-03109-1/AI: Bundesamt für Sicherheit in der Informationstechnik, BSI TR-03109-1 Anlage I: CMS-Datenformat für die Inhaltsdatenverschlüsselung und -signatur, 2013

BSI TR-03109-1/AII: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-03109-1 Anlage II "COSEM/HTTP Webservices" (Version 1.0), 2012

BSI TR-03109-1/AIIIa: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-03109-1, Anlage III: Feinspezifikation „Drahtlose LMN-Schnittstelle“ - Teil a: „OMS Specification Volume 2, Primary Communication“, 2013

BSI TR-03109-1/AIIIb: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-03109-1, Anlage III: Feinspezifikation „Drahtlose LMN-Schnittstelle“ - Teil b: „OMS Technical Report Security“, 2013

BSI TR-03109-1/AIVa: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-03109-1, Anlage IV: Feinspezifikation „Drahtgebundene LMN-Schnittstelle“ Teil a: „HDLC für LMN“, 2013

BSI TR-03109-1/AIVb: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-03109-1, Anlage IV: Feinspezifikation „Drahtgebundene LMN-Schnittstelle“ - Teil b: „SML – Smart Message Language“, 2013

BSI TR-03109-1/AV: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-03109-1, Anlage V: Anforderungen zum Betrieb beim Administrator, 2013

BSI TR-03109-1/AVI: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-03109-1, Anlage VI: Betriebsprozesse,

BSI TR-03109-2: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-03109-2 "Smart Meter Gateway - Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls" (Version 1.0), 2013

BSI TR-03109-3: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-03109-3 "Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen" (Version 1.1), 2014

BSI TR-03109-4: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-03109-4 "Smart Metering PKI - Publik Key Infrastruktur für Smart Meter Gateways" (Version 1.0), 2013

BSI TR-03109-TS-1: (Entwurfsphase: T-Systems), Testspezifikation BSI TR-03109-TS-1 "Testspezifikation zur Interoperabilitätsprüfung von Kommunikationseinheiten intelligenter Messsysteme gemäß BSI TR-03109-1" (Version: Entwurf), 2014

BSI TR-03111: Bundesamt für Sicherheit in der Informationstechnik, Technical Guideline - Elliptic Curve Cryptography, 2012

BSI TR-03116-3: Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR-03116-3: Kryptographische Vorgaben für Projekte der Bundesregierung - Teil 3 - Intelligente Messsysteme, 2014

EN 13757-1: CEN (DIN), Kommunikationssysteme für Zähler und deren Fernablesung - Teil 1: Datenaustausch, 2003

EN 13757-3: CEN (DIN), Kommunikationssysteme für Zähler und deren Fernablesung - Teil 3: Spezieller Application Layer, DIN EN 13757-3:2005-02, 2005

EN 13757-4: CEN (DIN), Kommunikationssysteme für Zähler und deren Fernablesung - Teil 4: Zählerauslesung über Funk (Fernablesung von Zählern im SRDBand von 868 MHz bis 870 MHz), 2011

ETSI EG 202 568: European Telecommunications Standards Institute, Methods for Testing and Specification (MTS);Internet Protocol Testing (IPT);Testing: Methodology and Framework, 2007

ETSI ES 202 553: European Telecommunications Standards Institute, Methods for Testing and Specification (MTS);TPLan: A notation for expressing Test Purposes, 2009

ETSI ETS 300 406: European Telecommunications Standards Institute, Methods for Testing and Specification (MTS);Protocol and profile conformance testing specifications;Standardization methodology, 1995

GW_PP: Bundesamt für Sicherheit in der Informationstechnik, Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP) "Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen" (Version 1.3, Certification-ID: BSI-CC-PP0073), 2014

IEC 62056-46: International Electrotechnical Commission, Electricity metering–Data exchange for meter reading, tariff and load control–Part 46: Data link layer using HDLC protocol, 2002

IEC 62056-5-3-8: International Electrotechnical Commission, Electricity metering–Data exchange for meter reading, tariff and load control–Part 5-3-8: Smart Message Language SML, 2012

IEC 62056-6-1: International Electrotechnical Commission, IEC 62056-6-1 "Electricity metering data exchange - The DLMS/COSEM suite - Part 6-1: COSEM Object Identification System (OBIS)", 2010

IEC 62056-6-2: International Electrotechnical Commission, Electricity metering–Data exchange for meter reading, tariff and load control–Part 6-2: Interface classes, FDIS IEC,Melbourne meeting, 2011

IEEE 802.3i: Institute of Electrical and Electronics Engineers, IEEE Std 802.3i-1990 (Clauses 13 and 14), 10 Mb/s UTP MAU, 10 BASE-T,

ISO/IEC 13239: ISO/IEC, Information technology - Telecommunications and information exchange between systems - High-level data link control (HDLC) procedures, 2002

ISO/IEC 9646-1: ISO/IEC, ISO/IEC 9646-1:1994 Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 1: General concepts, 1994

ISO/IEC 9646-1: ISO/IEC, Information Technology - Open Systems Interconnection - Conformance Testing Methodology and Framework - Part 1: General concepts, 1992

ISTQB®-Glossar: International Software Testing Qualification Board, ISTQB®/GTB Standardglossar der Testbegriffe "Deutsch - Englisch" (Version 2.3), 2014

M441-TR: CEN/CENELEC/ETSI, Functional Reference Architecture for Communications in Smart Metering Systems "Technischer Bericht - Funktionale Referenzarchitektur für die Kommunikation in intelligenten Messsystemen" (Version: Final Draft 50572), 2011

OMS-TR-01: OMS, Open Metering System Technical Report 01-Security, Issue 1.1.0, 2012

RFC2616: W3C, RFC 2616 "Hypertext Transfer Protocol -- HTTP/1.1", 1999

RFC4366: Internet Engineering Task Force, Transport Layer Security (TLS) Extensions, 2006

RFC4492: Internet Engineering Task Force, Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS), 2006

RFC5077: Internet Engineering Task Force, Transport Layer Security (TLS) Session Resumption without Server-Side State, 2008

RFC5083: Internet Engineering Task Force, Cryptographic Message Syntax (CMS) - Authenticated-Enveloped-Data Content Type, 2007

RFC5246: Internet Engineering Task Force, The Transport Layer Security (TLS) Protocol Version 1.2, 2008

RFC5639: Internet Engineering Task Force, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, 2010

RFC5652: Internet Engineering Task Force, Cryptographic Message Syntax (CMS), 2009

RFC7027: Internet Engineering Task Force, Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS), 2013

XSD-COD: DKE, XSD-COD "Entwurf des XSD Schemas für COSEM Datentypen nach DLMS Contribution 050, basierend auf asn.1" (Version 0.2), 2014
XSD-COR: DKE, XSD-COR "Entwurf des XSD Schemas für RESTful COSEM Webservices des DKE AK461.0.143" (Version 0.2), 2014

2824

Glossar und Abkürzungsverzeichnis

Dieser Anhang hat informativen Charakter.

Als Glossar und Abkürzungsverzeichnis dienen gleichlautend wie für [BSI TR-03109-1] Kapitel 7.2 des Schutzprofils [GW_PP] sowie Anhang B von [M441-TR]. Diese Dokumente sind in englischer Sprache verfasst. Alle dort aufgeführten Begriffe gelten in der dort beschriebenen Bedeutung auch für das vorliegende Dokument.

Glossar

Folgende, nicht in Kapitel 1.4 bereits aufgeführten Begriffe werden in [BSI TR-03109-TS-1] zusätzlich in der unten definierten Bedeutung benutzt.[48]

Begriff	Erläuterung
Testart	[ISTQB®-Glossar]: Eine Gruppe von Testaktivitäten, mit der Absicht, eine Komponente oder ein System auf einige zusammenhängende Qualitätsmerkmale zu prüfen. Eine Testart ist auf ein bestimmtes Testziel fokussiert, wie z. B. Zuverlässigkeitstest, Regressionstest, Benutzbarkeitstest. Die Testart kann sich auch auf eine oder mehrere Teststufen oder -phasen beziehen.
Testelement	[ISTQB®-Glossar]: Das einzelne Element, das getestet wird. Gewöhnlich existieren ein Testobjekt und viele Testelemente.
Testfallkette	Die Zusammenstellung (Aggregation) mehrerer Testfälle für den Test einer Komponente oder eines Systems, bei der Nachbedingungen des einen Tests als Vorbedingungen des folgenden Tests genutzt werden können.
Testobjekt	[ISTQB®-Glossar]: Die Komponente oder das System, welches getestet wird.
Testszenario Testablauf-spezifikation	[ISTQB®-Glossar]: Ein Dokument, das eine Folge von Schritten zur Testausführung festlegt. Auch bekannt als Testskript oder Testdrehbuch.
Testtreiber	[ISTQB®-Glossar]: Ein Testwerkzeug, das eine zu testende Komponente/ein System aufruft und/oder steuert.
Testverfahren	[ISTQB®-Glossar]: Eine Kombination von Tätigkeiten zum systematischen Erzeugen eines Testproduktes. Testverfahren sind unter Anderem verfügbar für: Testschätzung, Fehlermanagement, Produktrisikoanalyse, Testentwurf, Testdurchführung und Reviews.

Tabelle 125: Glossarbegriffe

48 Für Begriffsdefinitionen mit normativem Charakter vgl. Kapitel1.4.

Abkürzungen

Abkürzung	Erläuterung
ATS	Abstract Test Suite
CMS	Cryptographic Message Syntax
DLMS	Device Language Message Specification
FNN	Forum Netztechnik/Netzbetrieb im VDE
ICS	Implementation Conformance Statement
IUT	Implementation under Test
LV	Letztverbraucher
PCO	Point of Control and Observation
PHY	Kurzbezeichnung für die physikalische Schicht des OSI-Modells
SecMod	Sicherheitsmodul eines SMGW (abgeleitet von der englischen Bezeichnung Security Module)
SM-PKI	Smart Metering - Public Key Infrastruktur
SUT	System under Test (Synonym für das Testobjekt verwendet)
TC	Test Case (Testfall)
TR	Technische Richtlinie
TS	Testspezifikation

Tabelle 126: Abkürzungen

Anlagen

Bezeichnung	Beschreibung: Dateiname (Speicherort)
A1	Beispieltestfall 1: `testcase_TLS_Handshake.xml` (in Archiv: `XML - Anlagen A - Beispiele.zip`)
A2	Beispieltestfall 2: `wake_up.xml` (in Archiv: `XML - Anlagen A - Beispiele.zip`)
B1	Schema-Beschreibung: `bsi_tr-03109-1.xsd` (in Archiv: `XML - Anlagen B - Struktur.zip`)
B2	Testsuite-XML-Datei: `main.xml` (in Archiv: `XML - Anlagen B - Struktur.zip`)
B3	Testfall-XML-Datei: `testcase.xml` (in Archiv: `XML - Anlagen B - Struktur.zip`)
B4	Vorbedingungsdefinition (XML-Datei): `preconditions.xml` (in Archiv: `XML - Anlagen B - Struktur.zip`)
B5	Testdaten (XML-Datei): testdata `.xml` (in Archiv: `XML - Anlagen B - Struktur.zip`)
B6	`Schnittstellen-Zuordnung (XML-Datei): interfaces.xml` (in Archiv: `XML - Anlagen B – Struktur.zip`)
B7	`Konfigurationsvorgaben (XML-Datei): testconfigurations.xml` (in Archiv: `XML - Anlagen B – Struktur.zip`)
C	Übersicht zu nicht oder nur eingeschränkt testbaren Anforderungen (Stand Oktober 2014): TR-03109-TS-1_TK_Anlage-C_Anforderungsunterdeckung.pdf
D	Übersicht Testelemente/Testelementgliederung 1. Ebene (Stand Dezember 2014): TR-03109-TS-1_TK_Anlage-D_TE-Gliederung.pdf

Tabelle 127: Anlagenübersicht