



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Technische Richtlinie BSI TR-03109-1

Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems

Version 1.1

Datum:2021-09-17, Commit:6b75fb88



Bundesamt für Sicherheit in der Informationstechnik

Postfach 20 03 63

53133 Bonn

E-Mail: smartmeter@bsi.bund.de

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

© Bundesamt für Sicherheit in der Informationstechnik 2021

Inhaltsverzeichnis

1.	Einleitung	1
1.1.	Vorwort	1
1.2.	Zielsetzung	2
1.3.	Zielgruppe	2
1.4.	Anwendungsbereich	2
1.5.	Fachlich zuständige Stelle	2
1.6.	Terminologie	3
1.7.	Aufbau der Technischen Richtlinie	3
1.8.	Übersicht über mitgeltende Anlagen	4
1.9.	Zusammenhang mit anderen Technischen Richtlinien	4
1.10.	Nachweispflicht zur Interoperabilität nach MsbG	4
1.11.	Versionshistorie	5
2.	Technische Einleitung	6
2.1.	Akteure am SMGW	6
2.2.	Schnittstellen und Funktionen des SMGW	7
2.3.	Interoperabilitätsmodell	11
3.	Anforderungen an die Kommunikationsverbindungen und Protokolle des SMGW	15
3.1.	Einleitung	15
3.2.	Vorgaben an die Kommunikationsverbindungen im WAN	15
3.3.	Vorgaben an die Kommunikationsverbindungen in das LMN	43
3.4.	Vorgaben an die Kommunikationsverbindungen in das HAN	50
4.	Messwertverarbeitung für Tarifierung, Bilanzierung und Netzzustandsdatenerhebung	73
4.1.	Einleitung	73
4.2.	Anwendungsfälle für Regelwerke	73
4.3.	Messwertverarbeitung mit Regelwerken	93
4.4.	Konfigurationsprofile	98
4.5.	Anforderungen an Berechtigungen	100
5.	Weitere Funktionale Anforderungen	103
5.1.	Zusammenspiel SMGW und Sicherheitsmodul	103
5.2.	Logdatenformat	108
5.3.	Inhaltliche Daten der Log-Klassen	110
5.4.	Eindeutige Geräte-Identifikation des SMGW	112
6.	Nicht-Funktionale Anforderungen	113
6.1.	Einleitung	113
6.2.	Versiegelung	113
6.3.	Einbau des Sicherheitsmoduls	114
	Literaturverzeichnis	115

Glossar	117
A. Abkürzungsverzeichnis	122
B. Changelog	124

Abbildungsverzeichnis

2.1. Einbettung des SMGW in seine Einsatzumgebung	7
2.2. Interoperabilitätsmodell für SMGW	13
2.3. Die zwei Dimensionen des Interoperabilitätsmodells	14
3.1. Sequenzdiagramm Kommunikationsszenario „MANAGEMENT“	22
3.2. Sequenzdiagramm Kommunikationsszenario „ADMIN-SERVICE“	23
3.3. Sequenzdiagramm Kommunikationsszenario „INFO-REPORT“	25
3.4. Sequenzdiagramm Kommunikationsszenario „NTP-HTTPS“	26
3.5. Sequenzdiagramm Kommunikationsszenario „NTP-TLS“	28
3.6. Sequenzdiagramm Kommunikationsszenario „TLSPROXY“	29
3.7. Sequenzdiagramm für Anwendungsfall und Kommunikationsszenario „WAKEUP“	30
3.8. Protokollstapel für die WAN-Kommunikation	36
3.9. Zeitsynchronisation zwischen SMGW und GWA-Zeitserver	41
3.10. Sequenzdiagramm für bidirektionale LMN-Kommunikation (LKS1)	46
3.11. Sequenzdiagramm für unidirektionale LMN-Kommunikation (LKS2)	47
3.12. Protokollstapel im LMN (für drahtlose und drahtgebundene Kommunikation)	49
3.13. Authentifizierung des Anschlussnutzers/ Servicetechnikers mittels HAN-TLS-Client-Zertifikat	55
3.14. Authentifizierung des Anschlussnutzers mittels Kennung und Passwort	56
3.15. Transparenter Kommunikationskanal initiiert durch CLS	56
3.16. Transparenter Kommunikationskanal initiiert durch aktiven EMT (über den GWA)	58
3.17. Sequenzdiagramm Transparenter Kommunikationskanal initiiert durch aktiven EMT	59
3.18. Transparenter Kanal initiiert durch das SMGW	62
3.19. Sequenzdiagramm Transparenter Kommunikationskanal initiiert durch SMGW	63
3.20. Absicherung der Kommunikation zwischen CLS und aktivem EMT	67
3.21. Protokollstapel für die HAN-Kommunikation	71
4.1. Beispiel für einen zeitvariablen Tarif mit zwei Tarifstufen (HT/NT)	77
4.2. Kumulation nach Behebung einer Empfangsstörung	78
4.3. Kumulation bei fehlerhafteten Messwerten	79
4.4. Übersicht der Messwertverarbeitung	93
4.5. Beziehungen zwischen den Profilen für die Konfiguration der Tarifierung	98

5.1.	Interaktion zwischen Gateway und Sicherheitsmodul beim TLS 1.2-Handshake 1/2	104
5.2.	Interaktion zwischen Gateway und Sicherheitsmodul beim TLS 1.2-Handshake 2/2	105
5.3.	Interaktion zwischen SMGW und SM bei der Inhaltsdatensicherung mit AES-CBC-CMAC	107

1. Einleitung

1.1. Vorwort

Die mit der rasanten Technologieentwicklung einhergehende Digitalisierung aller gesellschaftlichen Lebensbereiche stellt Staat, Wirtschaft und unsere Gesellschaft vor große Herausforderungen. Anstelle von wenigen Großkraftwerken wird eine Vielzahl von kleinen, dezentralen *Erzeugungsanlagen*, Anlagen zur Speicherung elektrischer Energie und flexiblen Verbrauchseinrichtungen in das intelligente Energienetz integriert werden. Weiterhin werden auch auf Verbraucherseite durch den Hochlauf der Elektromobilität sowie die Wärmewende steuerbare und flexible Kundeneinrichtungen entstehen. Flexibilität im zukünftigen Smart Grid ist nötig, um Erzeugung und *Verbrauch* aufeinander abzustimmen.

Um diese Ziele erfolgreich umsetzen zu können, muss das Verteilnetz auf Basis intelligenter Messsysteme stufenweise digitalisiert werden. Denn durch die Verwendung von intelligenten Messsystemen – und der damit einhergehenden Verwendung von zertifizierten Smart-Meter-Gateways (SMGW) – werden wichtige Systeme des Energienetzes über eine sichere Kommunikationsinfrastruktur vernetzt. Zugleich wird Cyber-Angriffen auf solche Systeme wirksam begegnet. Durch den Einsatz von Smart-Meter-Gateways können *Netzzustandsdaten* erhoben werden, sodass mehr Transparenz über die Leistungsflüsse im Verteilnetz entsteht. Zudem können flexible Verbrauchseinrichtungen (Wärmepumpen, Elektromobile usw.), Anlagen zur Speicherung elektrischer Energie und dezentrale Erzeugungsanlagen über das Smart-Meter-Gateway gesteuert und somit netz- und marktdienlich eingesetzt werden.

Im Zuge der Energiewende gehören Smart-Meter-Gateways damit zu den Schlüsseltechnologien und sind ein gutes Beispiel dafür, welchen Einfluss digitale und vernetzte Technologien auf den Alltag der Verbraucher haben werden und wie wichtig in diesem Zusammenhang die frühzeitige Umsetzung von hohen Vorgaben zum Datenschutz und zur IT-Sicherheit sind („Security & Privacy by Design“). Aufgabe und Anspruch des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist es, die Informationssicherheit in der Digitalisierung zu gestalten und zu gewährleisten, damit die Anwender von den Vorzügen dieser innovativen Technologien profitieren können. Nur wenn Staat, Wirtschaft sowie Bürgerinnen und Bürger auf den Schutz ihrer Daten vertrauen können und ihre IT-Systeme gegen zunehmende Bedrohungen ausreichend geschützt sehen, wird diese digitale Transformation gelingen und deren Potential auch voll ausgeschöpft werden können.

In Zusammenhang mit den technischen Standards des BSI schafft das Messstellenbetriebsgesetz (MsbG) verbindliche Rahmenbedingungen für den sicheren und datenschutzkonformen Einsatz von intelligenten Messsystemen in unterschiedlichen Einsatzbereichen und ermöglicht damit einen stufenweisen Rollout mit sukzessiver Weiterentwicklung der Systeme für neue Anwendungsfälle.

Ein sicherer Betrieb digitaler Infrastruktur und die Realisierung der im MsbG genannten Anwendungen mit dieser Infrastruktur ist nur über ein Zusammenwirken von Hardware-Komponenten vor Ort, Software und den informationstechnischen Systemen (sog. Backend-Systeme) von Gateway-Administratoren und Nutzern der intelligenten Messsysteme (Messstellenbetreiber, Lieferanten, Netzbetreiber, usw.) möglich. Besonders Visualisierungslösungen und Tarifierungslogiken – gerade solche für komplexe variable Tarife – werden oftmals nur in Backend-Systemen zu realisieren sein. Gleiches gilt für besondere Smart-Grid-Anwendungen wie Priorisierungsmöglichkeiten nach § 21 MsbG, die stets im arbeitsteiligen Zusammenwirken zwischen Backend und Smart-Meter-Gateway realisiert werden. Der systemische Ansatz des MsbG unterstreicht, dass intelligente Messsysteme und insbesondere das Smart-Meter-Gateway als zentrale Kommunikationsplattform ihre Aufgaben nur im arbeitsteiligen Zusammenspiel mit den Backendsystemen erfüllen können. Das MsbG schafft damit zukunftsorientierte Systemgrundlagen und keine abschließenden Systemvorgaben.

Im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) entwickelt das BSI daher Anforderungen an vertrauenswürdige Produktkomponenten (SMGW mit integriertem Sicherheitsmodul), deren si-

cheren IT-Betrieb (Administration) und an die vertrauenswürdige Kommunikationsinfrastruktur (Smart-Metering-Public-Key-Infrastruktur), siehe auch ▶Abschnitt 1.9.

Durch den Start des Rollouts in 2020 können das Potential der sicheren Gateway-Kommunikationsplattform bereits umfangreich genutzt und wertvolle Erfahrungen für die Weiterentwicklung der technischen Standards gesammelt werden. Gemeinsam mit dem BMWi hat das BSI bereits eine Standardisierungsstrategie zur sektorübergreifenden Digitalisierung der Energiewende erarbeitet und veröffentlicht (sog. "BMWi-BSI-Roadmap"). Auf ihrer Basis können gemeinsam mit den Verbänden, Partnerbehörden und den Unternehmen der Energiewirtschaft die wesentlichen technischen Weichenstellungen ("Technische Eckpunkte") und die daraus resultierenden Anforderungen für ein sicheres, intelligentes Energienetz (Smart Grid) der Zukunft festgelegt werden. Durch diesen erfolgreich aufgesetzten Branchendialog können stetig aktuelle Trends und Innovationen zielgerichtet erfasst und die Gateway-Technologie kontinuierlich in weiteren Einsatzbereichen stufenweise fortentwickelt werden.

1.2. Zielsetzung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat diese Technische Richtlinie mit dem Ziel erstellt, Mindestanforderungen an die Funktionalität und Interoperabilität zu beschreiben, die eine Kommunikationseinheit eines intelligenten Messsystems erfüllen muss und die sich zumeist unmittelbar oder mittelbar aus dem Messstellenbetriebsgesetz ergeben.

Die BSI TR-03109-1 ergänzt das Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems [PP-0073] um Anforderungen an die Funktionalität, die Kommunikationsverbindungen und Protokolle, die Messwertverarbeitung für die Tarifierung und Netzzustandsdatenerhebung, die Inhaltsdatenverschlüsselung, Signierung, Absicherung der Kommunikation und Authentifizierung der Datennutzer sowie die kryptographischen Verfahren (vgl. § 22 Abs. 4 MsbG).

Die Kommunikationseinheit eines intelligenten Messsystems ist das sogenannte Smart-Meter-Gateway (SMGW). Mit "TR" wird im Folgenden die BSI TR-03109-1 bezeichnet, sofern nicht explizit eine andere Technische Richtlinie referenziert wird.

1.3. Zielgruppe

Die TR richtet sich in erster Linie an Hersteller von SMGW. Die Konformität eines Produktes zu den Anforderungen dieser TR muss durch den SMGW-Hersteller durch eine Prüfung gemäß einer Prüfspezifikation des BSI nachgewiesen werden und wird durch ein Zertifikat des BSI abschließend bestätigt.

1.4. Anwendungsbereich

Die TR betrachtet SMGW und deren Schnittstellen zu den Kommunikationspartnern, die im jeweiligen Einsatzbereich der SMGW erforderlich sind.

1.5. Fachlich zuständige Stelle

Fachlich zuständig für die Fortentwicklung der TR ist das BSI.

Anschrift: Bundesamt für Sicherheit in der Informationstechnik
Referat DI 21 - Cyber-Sicherheit für die Digitalisierung der Energiewirtschaft
Postfach 20 03 63 222
53133 Bonn
E-Mail: SmartMeter@bsi.bund.de

Anmerkungen zu der Technischen Richtlinie können an die o.a. Anschrift oder E-Mail-Adresse gerichtet werden.

1.6. Terminologie

Es kann zwischen normativen und informativen Inhalten unterschieden werden. Im Rahmen der normativen Inhalte werden die in Großbuchstaben geschriebenen deutschen Schlüsselwörter auf Basis von [RFC2119] verwendet:

- **MUSS / MÜSSEN** bedeutet, dass es sich um eine normative Anforderung handelt.
- **DARF NICHT / DARF KEIN / DÜRFEN NICHT / DÜRFEN KEIN** bezeichnet den normativen Ausschluss einer Eigenschaft.
- **SOLL / SOLLEN** beschreibt eine dringende Empfehlung. Abweichungen zu diesen Festlegungen müssen begründet werden.
- **KANN / KÖNNEN / DARF / DÜRFEN** bedeutet, dass die Eigenschaften fakultativ oder optional sind.

Die Kapitel der Technischen Richtlinie sind grundsätzlich als normativ anzusehen. Informative Inhalte werden explizit gekennzeichnet.

Zur Definition von Anforderungen an eine Implementierung werden die folgenden Begriffe und Notationen verwendet:

Begriff	Beschreibung
REQ	Requirement. Beschreibt eine Anforderung an die Implementierung des Herstellers und identifiziert sie mittels einer eindeutigen ID. Die Requirement-ID setzt sich zusammen aus einer Abkürzung der fachlichen Einordnung (z.B. NFA für Nicht-Funktionale Anforderungen), der Kennzeichnung REQ und einer in der Regel in Zehnerschritten fortlaufenden Nummer. Es werden Schlüsselwörter verwendet, um zwischen normativen Anforderungen (MUSS), normativen Ausschlüssen (DARF NICHT), dringenden Empfehlungen mit Notwendigkeit einer Begründung bei Abweichung (SOLL) und optionalen Anforderungen (KANN / DARF) zu unterscheiden.
ICS	Implementation Conformance Statements. ICS definieren, welche zusätzlichen Informationen der Hersteller über die Implementierung des SMGW im Rahmen einer Produktzertifizierung deklarieren MUSS. Über ein ICS kann beispielsweise angegeben werden, ob der Hersteller eine bestimmte KANN-Anforderung erfüllt oder nicht. Ein ICS verfügt ebenso wie ein Requirement über eine eindeutige ID, welche sich analog zusammensetzt (mit der Kennzeichnung ICS).

Tabelle 1.1 Anforderungstypen

1.7. Aufbau der Technischen Richtlinie

Beginnend mit Kapitel ▶2 „Technische Einleitung“ wird in einer kurzen Einführung dargelegt, wie die Einbettung des SMGW in die Gesamtarchitektur eines Smart Metering Systems zu sehen ist. Darauf aufbauend werden die funktionalen Aspekte des SMGW skizziert. Zuvor werden die Akteure benannt, die in verschiedenen Rollen mit dem SMGW kommunizieren können.

Das folgende Kapitel ▶3 „Anforderungen an die Kommunikationsverbindungen und Protokolle des SMGW“ macht Vorgaben zur Sicherung aller Kommunikationsbeziehungen des SMGW und stellt Mindestforderungen in Bezug auf die zu unterstützenden Anwendungsfälle, *Kommunikationsszenarien* und Protokolle.

Kapitel ▶4 beschreibt die „Messwertverarbeitung für *Tarifierung*, *Bilanzierung* und *Netzzustandsdatenerhebung*“ sowie die *Auswertungsprofile* mit deren Hilfe das Rollen- und Rechtmanagement zum Zugriff auf die Messwerte im SMGW festgelegt wird.

In Kapitel ▶5 „Weitere Funktionale Anforderungen“ werden Anforderungen an das SMGW spezifiziert, die über die in Kapitel ▶4 beschriebenen Funktionen hinaus von Bedeutung sind.

Nicht-funktionale Anforderungen bzw. Eigenschaften, die das SMGW zusätzlich aufweisen muss, finden sich in Kapitel ▶6 „Nicht-Funktionale Anforderungen“.

1.8. Übersicht über mitgeltende Anlagen

- Die Detailspezifikationen zur TR-03109-1 [DS] regeln Details der Implementierung, beispielsweise zur Struktur des Wake-Up-Pakets und der Zertifikatsprofile und schließen Interpretationslücken in referenzierten Universalspezifikationen. Normative Anforderungen sind in den Detailspezifikationen entsprechend der Vorgaben dieser TR mit eindeutigen Bezeichnern gekennzeichnet.
- Die Anlage I: CMS-Datenformat für die Inhaltsdatenverschlüsselung und -signatur [TR-03109-1-I] beschreibt weitere Details zur Nutzung von CMS. Diese Anlage ist **normativ** und wird künftig in der Detailspezifikation zur TR-03109-1 aufgehen.
- Die Anlage II: COSEM/HTTP Webservices ist entfallen. Sie wurde durch Kapitel 6 der Detailspezifikation zur TR-03109-1 ersetzt.
- Die Anlage IIIa: Feinspezifikation "Drahtlose LMN-Schnittstelle" Teil a: "OMS Specification Volume 2, Primary Communication" ist entfallen. Sie wurde durch Kapitel 9 der Detailspezifikation zur TR-03109-1 ersetzt.
- Die Anlage IIIb: Feinspezifikation "Drahtlose LMN-Schnittstelle" Teil b: "OMS Technical Report Security" ist entfallen. Sie wurde durch Kapitel 9 der Detailspezifikation zur TR-03109-1 ersetzt.
- Die Anlage IVa: Feinspezifikation "Drahtgebundene LMN-Schnittstelle" Teil a: "HDLC für LMN" ist entfallen. Sie wurde durch Kapitel 8 der Detailspezifikation zur TR-03109-1 ersetzt.
- Die Anlage IVb: Feinspezifikation "Drahtgebundene LMN-Schnittstelle" Teil b: "SML – Smart Message Language" ist entfallen. An den relevanten Stellen wurde stattdessen ein Verweis auf [VDE0418-63-9] eingefügt.
- Die Anlage V: Anforderungen zum Betrieb beim Administrator ist entfallen. Die dortigen Anforderungen wurden in die Richtlinie [TR-03109-6] überführt.
- Die Anlage VI: Betriebsprozesse [TR-03109-1-VI] ist **informativ** und soll künftig in der TR-03109-1 aufgehen.
- Die Anlage VII: Interoperabilitätsmodell und Geräteprofile für Smart-Meter-Gateways ist entfallen. Die dortigen Anforderungen wurden in die TR-03109-1 überführt.
- Die Anlage VIII: Lebenszyklus [TR-03109-1-VIII] ist **informativ** und beschreibt den Lebenszyklus von der Entwicklung bis zur Verschrottung.

1.9. Zusammenhang mit anderen Technischen Richtlinien

- Die Richtlinie [TR-03109-2] beschreibt das Sicherheitsmodul des SMGW und die von ihm bereitzustellende Funktionalität.
- Die Richtlinie [TR-03109-3] legt Vorgaben an die einzusetzenden kryptographischen Verfahren fest.
- Die Richtlinie [TR-03109-4] spezifiziert die Architektur sowie die Mindestanforderungen an Interoperabilität und Sicherheit der Smart-Metering-PKI (SM-PKI).
- Die Richtlinie [TR-03109-6] beschreibt die Anforderungen an den Smart-Meter-Gateway-Administrator (GWA).

Weitere referenzierte Literatur, wie IETF RFC sind im Literaturverzeichnis am Ende dieses Dokumentes beschrieben.

1.10. Nachweispflicht zur Interoperabilität nach MsbG

Der Zeitpunkt des Beginns der Nachweispflicht zur Interoperabilität gemäß § 24 Abs. 1 Satz 3 wurde durch das Bundesamt für Sicherheit in der Informationstechnik auf den 31. Januar 2022 festgelegt. Der Zeitpunkt wurde gemäß § 27 MsbG im Ausschuss Gateway-Standardisierung in der Sitzung vom 09. August 2021 bekannt gemacht.

1.11. Versionshistorie

Version	Datum	Beschreibung
0.20	10.10.2011	Veröffentlichung Draft 1
0.50	25.05.2012	Veröffentlichung Draft 2
1.0 RC	21.12.2012	Veröffentlichung Version 1.0 (Release Candidate)
1.0	18.03.2013	Veröffentlichung Version 1.0
1.0.1	16.01.2019	Veröffentlichung Version 1.0.1 - Anlage VII ergänzt
1.1	17.09.2021	finale Version nach Abstimmung im Ausschuss Gateway-Standardisierung, Grundlegende Überarbeitung zur Vorversion, s. Changelog

Tabelle 1.2 Versionshistorie

2. Technische Einleitung

Das Kapitel beschreibt die Funktionalität der Kommunikationseinheit eines intelligenten Messsystems (SMGW) und ihre Einbettung in das technische und organisatorische Umfeld.

Des Weiteren beschreibt dieses Kapitel die mit dem SMGW kommunizierenden Akteure (► Abschnitt 2.1).

2.1. Akteure am SMGW

Zur Beschreibung der Funktionalität des SMGW ist es erforderlich, verschiedene Akteure zu benennen, die im Kontext dieser Technischen Richtlinie mit dem SMGW kommunizieren. Die Notwendigkeit und Definition jedes Akteurs ergibt sich dabei entweder direkt aus dem Rechtsrahmen oder als technische Notwendigkeit zur Erfüllung von Anwendungsfällen, die durch den Rechtsrahmen gefordert werden. Die hier definierten Akteure sind im Rahmen des SMGW-Betriebs relevant. In anderen Phasen des Lebenszyklus können weitere Rollen involviert sein. Diese werden in der entsprechenden Anlage zum Lebenszyklus benannt.

Folgende Akteure werden in der Technischen Richtlinie für den SMGW-Betrieb unterschieden:

2.1.1. Anschlussnutzer

Technischer Akteur am SMGW, der elektrische Energie, thermische Energie, Gas oder Wasser bezieht oder erzeugt und zur Nutzung des Netzanschlusses berechtigt ist. Der *Anschlussnutzer* verwendet zur Interaktion mit dem SMGW ein Kommunikationsgerät (z.B. Display). Der technische Akteur Anschlussnutzer ist beispielsweise ein Letztverbraucher oder Anlagenbetreiber gemäß [MsbG]. In früheren Versionen dieses Dokuments wurde und in referenzierten Dokumenten wird der Anschlussnutzer auch als Letztverbraucher bezeichnet. Gleiches gilt für Kompositionen wie dem Letztverbraucher-Log.

Mithilfe einer Transparenz- und Displaysoftware nach [MessEV] kann der Anschlussnutzer eine Rechnungsprüfung durchführen. Die dazu notwendigen Daten werden dem Anschlussnutzer vom SMGW über die HAN-Schnittstelle oder vom Messstellenbetreiber (MSB) über eine API bereitgestellt.

2.1.2. Smart-Meter-Gateway-Administrator

Der Smart-Meter-Gateway-Administrator (GWA) ist für das SMGW die vertrauenswürdige Instanz und übernimmt dessen Konfiguration, Überwachung und Steuerung. Er erstellt und administriert die in das SMGW eingespielten Profile zur sicheren Anbindung von Kommunikationspartnern, zur Messwertverarbeitung (Erfassung, Speicherung, Verarbeitung und Versand), zur Verwaltung SMGW-interner Prozesse und führt bei Bedarf die Aktualisierung der SMGW-Firmware durch. Der GWA hat keine Einsicht in die Messwerte.

GWA kann sowohl die Organisation, als auch das von der Organisation verwendete Kommunikationssystem (z.B. Backend) bezeichnen.

2.1.3. Berechtigte Externe Marktteilnehmer (Authorized External Entity)

Externe Marktteilnehmer (EMT) sind aus Sicht des SMGW alle Teilnehmer im Weitverkehrsnetz mit Ausnahme des GWA, mit denen das SMGW eine Kommunikation zum Austausch von Daten aufnehmen kann. Hierunter fallen z.B. der Verteilnetzbetreiber (VNB), der Messstellenbetreiber (MSB), der Energielieferant (LF) und sonstige autorisierte Dienstleister.

Berechtigte EMT werden in der SM-PKI Policy [SM-PKI-CP] weiter differenziert in passive EMT, die den TLS-Proxy nicht nutzen dürfen und Daten nur vom SMGW empfangen und aktive EMT, die über den TLS-Pro-

xy des SMGW Informationen mit nachgelagerten Geräten (Controllable Local Systems) austauschen und auf diese einwirken dürfen.

EMT kann sowohl die Organisation, als auch das von der Organisation verwendete Kommunikationssystem (z.B. Backend) bezeichnen.

2.1.4. Zähler/Messeinrichtungen

Messeinrichtungen (eng. Meter, MTR) im Lokalen Metrologischen Netzwerk (LMN) dienen der Erfassung von *Verbrauch* und Erzeugung von *Stoff- oder Energiemengen*. Erhobene Messwerte werden von der Messeinrichtung an das SMGW übermittelt.

2.1.5. Steuerbare lokale Systeme (Controllable Local Systems)

Controllable Local Systems (CLS) sind Systeme mit IT-Komponenten an der HAN-Schnittstelle des Anschlussnutzers, die nicht zum Intelligenten Messsystem gehören, aber das SMGW für bestimmte Kommunikationszwecke verwenden. CLS reichen beispielsweise von lokalen *Erzeugungsanlagen* über steuerbare Verbraucher bis zu Heimautomatisierungsanwendungen.

2.1.6. Servicetechniker

Der Servicetechniker (SRV) des GWA kann am Einsatzort des SMGW im Wirkbetrieb eine lokale Diagnose-schnittstelle am SMGW nutzen, um lesenden Zugriff auf das System-Logbuch und weitere Diagnosedaten zu erhalten sowie das Gerät in engen Grenzen zu parametrieren. SRV kann sowohl die Person, als auch das von der Person verwendete Kommunikationsgerät (z.B. Diagnosegerät) bezeichnen.

2.2. Schnittstellen und Funktionen des SMGW

Abgeleitet von der Systemarchitektur, die auf den Vorgaben des Schutzprofils [PP-0073] beruht, muss ein SMGW mindestens drei physische Schnittstellen bereitstellen, wie in ►Abbildung 2.1 dargestellt.

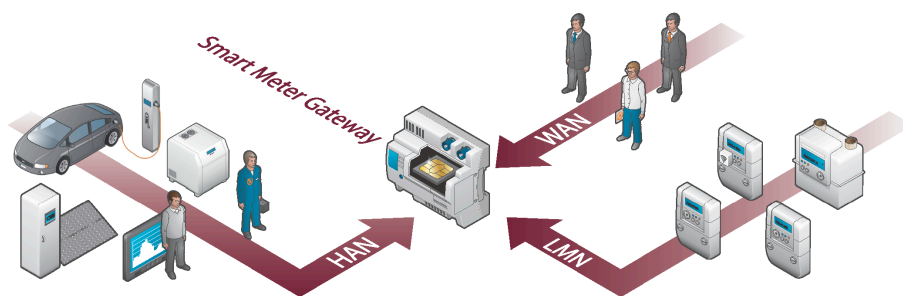


Abbildung 2.1. Einbettung des SMGW in seine Einsatzumgebung

Folgende Kommunikationsbereiche werden betrachtet:

- **Lokales metrologisches Netz (Local Metrological Network, LMN):** Im LMN kommuniziert das SMGW mit den angebotenen Messeinrichtungen für Stoff- und Energiemengen (Gas, Wasser, thermische Energie und Elektrizität) eines oder mehrerer Anschlussnutzer. Die Messeinrichtungen kommunizieren ihre Messwerte über das LMN an das SMGW.

- **Weitverkehrsnetz (Wide Area Network, WAN):** Im WAN kommuniziert das SMGW mit dem GWA und den EMT.
- **Heimnetz (Home Area Network, HAN):** Im HAN eines oder mehrerer Anschlussnutzer kommuniziert das SMGW mit den steuerbaren Energieverbrauchern bzw. Energieerzeugern (CLS, also z.B. private Ladeeinrichtungen, Kraft-Wärme-Kopplungs- oder Photovoltaik-Anlagen). Des Weiteren stellt das SMGW Daten sowohl für den Anschlussnutzer als auch für den Servicetechniker bereit.

Das SMGW kommuniziert intern mit seinem Sicherheitsmodul (SM), das als Common Criteria (CC)-zertifizierte Teilkomponente (s. [PP-0077]) kryptographische Operationen und einen sicheren Schlüssel- und Zertifikatsspeicher zur Verfügung stellt.

Die Hauptfunktionalität des SMGW besteht in der Speicherung der aus dem LMN empfangenen Messwerte, deren Verarbeitung gemäß konfigurierter Verarbeitungsprogramme und der Versendung der verarbeiteten Informationen an berechnete EMT im WAN. Diese Funktionalitäten sind in der Regel auch von Relevanz nach [MessEG]/[MessEV]. Informationen können durch das SMGW sternförmig an die jeweiligen Adressaten im WAN direkt verteilt werden, aber auch eine indirekte Verteilung über einen bestimmten Marktakteur wird ermöglicht.

Daneben bietet das SMGW Funktionen für Anschlussnutzer bzw. Servicetechniker, damit diese an der HAN-Schnittstelle Verbrauchsdaten bzw. Systeminformationen abrufen können. Für im HAN angeschlossene steuerbare Systeme (CLS) fungiert das SMGW als TLS-Proxy-Server: TLS-geschützte Kommunikationskanäle in Richtung CLS und in Richtung EMT werden im SMGW terminiert und das SMGW übernimmt die Weiterleitung der jeweils empfangenen Daten.

Gemäß [PP-0073] erfüllt das SMGW die Aufgaben einer Firewall und separiert die angebotenen Netze voneinander. Als dezentraler Speicher personenbezogener Informationen, die nur gemäß vertraglich vereinbarten Regelungen an berechnete Parteien versendet werden, stellt das SMGW Datenschutz und Datensicherheit für den Anschlussnutzer sicher.

2.2.1. Funktionen des SMGW für das lokale metrologische Netz

Das SMGW kommuniziert mit *Zählern* im lokalen metrologischen Netz und ist für den Empfang, die Verarbeitung und Speicherung von Messwerten und ggf. Netzzustandsdaten verantwortlich. Die lokal angeschlossenen Zähler werden dem SMGW in Form von entsprechenden *Zählerprofilen* durch den GWA bekannt gemacht (► Abschnitt 4.4.2).

Die sichere Kommunikation mit den Zählern erfolgt mit Hilfe der in ► Abschnitt 3.3 festgelegten Protokolle.

Erfassung, Zeitstempelung, Tarifierung und Speicherung von Messwerten

Die von den angeschlossenen Zählern im LMN übermittelten Daten können sowohl Verbrauchswerte als auch Angaben über in das Netz eingespeiste Energiemengen (z.B. bei Photovoltaikanlage, Blockheizkraftwerk) sein. Zusätzlich können weitere netzbetriebsrelevante Parameter wie bspw. Netzspannung, Frequenz, Phasenwinkel, die ggf. von einem Zähler bereitgestellt werden, vom SMGW aufgenommen werden. Folgende Verarbeitungsschritte werden vom SMGW an der LMN-Schnittstelle durchgeführt:

1. Das SMGW empfängt oder ruft in regelmäßigen Zeitabständen die Messwerte der lokal angeschlossenen Zähler ab. Das SMGW empfängt die Messwerte verschlüsselt und integritätsgesichert.
2. Das SMGW führt die Zeitstempelung empfangener Messwerte mithilfe der Systemuhr durch und speichert die Messwerte nach erfolgreicher Entschlüsselung und Integritätsprüfung in *Messwertlisten*.
3. Aus bestimmten Messwerten ermittelt das SMGW mit Hilfe eines *Regelwerks* abgeleitete Messwerte und versendet diese verarbeiteten Werte an berechnete EMT.

Der Vorgang der Zuordnung von Energie- oder Stoffmengen zu einer *Tarifstufe* wird in dieser TR als *Tarifierung* bezeichnet (► Abschnitt 4.3.3).

Das SMGW unterliegt wegen der durchgeführten Zeitstempelung, Tarifierung und Speicherung der *abrechnungsrelevanten Messwerte* (Messwerte zur Verwendung im geschäftlichen Verkehr) dem Eichrecht.

2.2.2. Funktionen des SMGW im Weitverkehrsnetz

Die Verbindung des SMGW zum GWA sowie zu den EMT geschieht über eine WAN-Verbindung.

Die Absicherung der Kommunikation erfolgt mittels der in ▶Abschnitt 3.2 festgelegten Protokolle.

Der GWA ist die vertrauenswürdige Instanz im WAN, die das SMGW konfiguriert und Wartungsarbeiten durchführt.

Folgende Funktionen des SMGW werden an der WAN-Schnittstelle sichtbar bzw. über die WAN-Schnittstelle angestoßen:

Übertragung der Messwerte anhand von Auswertungs- und WAN-Kommunikationsprofilen

Im SMGW werden vom GWA Regelwerke in Form von *Auswertungsprofilen* hinterlegt (▶Abschnitt 4.4.3 dieses Dokuments und in [PP-0073]), die die Weiterverarbeitung der empfangenen Informationen beschreiben. Nach der Verarbeitung erfolgt die Auslieferung der Daten an berechnete EMT im WAN und nach Ablauf der erforderlichen Aufbewahrungszeiten deren Löschung. Die Verbindungsparameter für die Übertragung der Messwerte hat das SMGW in *Kommunikationsprofilen* gespeichert.

Pseudonymisierung

Ist es aus Gründen des Datenschutzes erforderlich die Identität des Anschlussnutzers zu verschleiern, so wird die im Datensatz enthaltene Identifikation des Zählers bei Bedarf durch ein Pseudonym ersetzt. Damit auch die Identität des sendenden SMGW unerkannt bleibt, müssen die Daten zusätzlich über einen Dritten (den GWA) an den Endempfänger vermittelt werden (▶Abschnitt 4.3.8).

Empfang von Administrations- und Konfigurationsinformationen

Das SMGW wird vom GWA konfiguriert und administriert. Dazu sendet der GWA Konfigurationsinformationen (▶Abschnitt 4.4) und Befehle, die vom SMGW empfangen und verarbeitet werden.

Firmware-Update

Das SMGW unterstützt einen Firmware-Update-Prozess, der eine oder mehrere vom SMGW Hersteller bereitgestellte Firmware-Dateien in das SMGW überträgt und nach erfolgreicher Validierung installiert. Den Befehl dazu erhält das SMGW vom GWA. Der Updateprozess selbst ist nach [PP-0073] „fail safe“ implementiert, so dass Prozessfehler während des Firmware-Updates nicht zum Ausfall des SMGW führen.

Wake-Up-Service

Das SMGW stellt einen Wake-Up-Service für den GWA bereit. Der GWA kann mithilfe des Wake-Up-Service das SMGW auffordern eine WAN-Kommunikationsverbindung aufzubauen. Beim Wake-Up-Service empfängt das SMGW ein spezielles vom GWA signiertes Datenpaket (▶Abschnitt 3.2.6.3). Nach erfolgreicher Verifikation dieses einzelnen Paketes baut das SMGW eine fest vorkonfigurierte Verbindung zum GWA auf. Dieser kann über die nun etablierte Verbindung weitere Administrationsbefehle ausführen.

Zeitsynchronisation

Das SMGW benötigt für seine Aufgaben eine gültige, vertrauenswürdige Uhrzeit. Dazu nutzt das SMGW eine Systemuhr, die regelmäßig synchronisiert wird.

Die Synchronisation der SMGW-Systemuhr mit einer zuverlässigen externen Zeitquelle geschieht gemäß den Vorgaben aus ▶Abschnitt 3.2.7

2.2.3. Funktionen des SMGW für das Home Area Network

Das SMGW stellt drei logische Schnittstellen im HAN bereit:

CLS-Schnittstelle (IF_GW_CLS)

Über die CLS-Schnittstelle des SMGW können steuerbare Komponenten im HAN (z.B. Photovoltaikanlagen, Wärmepumpen) gesicherte Kommunikationsverbindungen mit einem EMT im WAN unterhalten (s.

[PP-0073]). Das SMGW stellt dazu jeweils TLS-gesicherte Verbindungen zur CLS-Komponente und zum steuerberechtigten EMT bereit, die es aufeinander abbildet. Spezifische Anwendungsfälle, die dem Monitoring oder der Steuerung der CLS-Komponente dienen, sowie *Kommunikationsszenarien* und die dazu notwendigen Protokolle, sind für das SMGW transparent (*Transparenter Kanal*).

Anschlussnutzer-Schnittstelle (IF_GW_CON)

Das SMGW bietet berechtigten Anschlussnutzern mit Hilfe der Anschlussnutzer-Schnittstelle (IF_GW_CON) nach [PP-0073] die Möglichkeit, im SMGW für den jeweiligen Anschlussnutzer gespeicherte und ihm zugeordnete Informationen abzurufen. Ein Zugriff auf diese Daten kann immer nur lesend und nach einer erfolgreichen Authentifizierung erfolgen.

Zur Auslesung und Visualisierung der Daten an dieser Schnittstelle kann ein dediziertes, kryptographisch gesichertes Display, ein lokaler PC mit der Transparenz- und Displaysoftware "TruDi" als Sichtanzeige nach [MessEG]/[MessEV] oder ein anderes (CLS-)Gerät im HAN Bereich genutzt werden, welches den kryptographisch gesicherten Datenstrom verarbeiten kann.

Servicetechniker-Schnittstelle (IF_GW_SRV)

Der Servicetechniker kann diese logische Schnittstelle nutzen, um z.B. *Konfigurationsprofile* und das System-Log einzusehen. Dies unterstützt ihn bei der Diagnose von Fehlersituationen. Darüber hinaus kann der Servicetechniker schreibend auf einzelne Konfigurationen zur Entstörung zugreifen. Ein solcher Zugriff setzt voraus, dass der SMGW-Hersteller die Sicherheit seiner Umsetzung im Rahmen der Zertifizierung nach Common Criteria nachgewiesen hat.

2.2.4. Weitere Funktionen des SMGW

Neben den bereits genannten Funktionalitäten hat das SMGW weitere Aufgaben zu erfüllen.

Nutzerverwaltung/Mandantenfähigkeit

Das SMGW muss die Messwerte von Zählern verschiedener Anschlussnutzer (bspw. in Mehrfamilienhäusern) erfassen und speichern können. Dazu hat das SMGW Mechanismen implementiert, um die Multi-Mandantenfähigkeit und die damit verbundenen Authentifizierungsanforderungen (s. [PP-0073]) umsetzen zu können.

Kryptographische Funktionen

Zur Erfüllung kryptographischer Funktionen wie Signaturerzeugung, Signaturprüfung und Generierung von Schlüsseln bzw. Zufallszahlen bedient sich das SMGW eines nach Common Criteria ([PP-0077]) zertifizierten Sicherheitsmoduls.

Das Sicherheitsmodul erfüllt die Anforderungen aus [TR-03109-2].

Protokollierung

Das SMGW protokolliert seine Aktionen in drei unterschiedlichen Log-Bereichen: im System-Log, Anschlussnutzer-Log sowie im *eichtechnischen Log*.

- **System-Log**

Jedes wichtige Ereignis (z.B. Fehlermeldungen, Ausfall der WAN-Verbindung, sicherheitsrelevante Ereignisse, Aktivitäten des GWA, etc.) im SMGW wird im System-Log protokolliert. Dieses Log kann nur von dem autorisierten GWA sowie dem autorisierten Servicetechniker vor Ort eingesehen werden. Die Informationen dienen dazu, den momentanen Status des SMGW zu erkennen und eventuelle Fehlerquellen oder Störungen zu identifizieren.

- **Anschlussnutzer-Log**

Alle Transaktionen des SMGW, z.B. das Versenden von Messwerten, und die den Anschlussnutzer betreffenden Aktivitäten des GWA werden in einem Anschlussnutzer-Log festgehalten. Ein authentifizierter und autorisierter Anschlussnutzer kann die ihn betreffenden

Informationen vom SMGW über die logische HAN-Schnittstelle für Anzeigeeinheiten abrufen und somit nachverfolgen, wer wann welche Daten erhalten hat, oder ob benutzerbezogene Daten (z.B. Profile) geändert bzw. hinzugefügt oder entfernt wurden.

Zur Wahrung der Vertraulichkeit und Integrität der personenbezogenen Protokolldaten ist niemandem außer dem jeweiligen Anschlussnutzer der Zugriff auf das persönliche Anschlussnutzer-Log erlaubt.

- **Eichtechnisches Logbuch**

Im eichtechnischen Logbuch werden nach [MessEG]/[MessEV] relevante Ereignisse aufgezeichnet. Außerdem erfolgt hier die Registrierung von Änderungen an nach [MessEG]/[MessEV] relevanten Parametern (z.B. das Stellen der Geräteuhr). Dieses Log kann nur vom autorisierten GWA abgerufen werden, um es zu den Zwecken der Befundprüfung und der Marktüberwachung den gemäß [MessEG]/[MessEV] zuständigen Stellen vollständig und signiert durch das SMGW zu übermitteln.

Aufbau und Struktur der Logs werden in ▶Abschnitt 5.2 festgelegt.

2.3. Interoperabilitätsmodell

In diesem Abschnitt werden die Grundlagen für ein gemeinsames Verständnis des Interoperabilitätsbegriffs geschaffen sowie der den Überlegungen zu den Interoperabilitätsanforderungen dieser TR zugrundeliegende Ansatz beschrieben.

Interoperabilität ist kein statischer Zustand, sondern ein Reifeprozess. Bei der Bestimmung des Reifegrades sind der Reifegrad dieser TR sowie der Reifegrad der Geräte logisch zu trennen. Die TR wird mittels eines fortlaufenden Entwicklungs- und Abstimmungsprozesses mit den beteiligten Akteuren fortgeschrieben, während die Geräte einen versionierten IST-Stand der TR nachbilden. Das Ziel dieses Abstimmungsprozesses ist es, die Interoperabilitätsanforderungen in der TR schrittweise zu vertiefen, um künftig die Austauschbarkeit der Geräte an den Schnittstellen zu ermöglichen. Im Sinne eines agilen Vorgehens müssen daher iterativ Anforderungen beschrieben, in der Praxis erprobt und unter Berücksichtigung der Erfahrungswerte weiter verfeinert werden.

2.3.1. Begriffsdefinitionen

Der Begriff der **Interoperabilität** wird von CEC/CENELEC/ETSI im Zusammenhang mit Smart-Metering wie folgt definiert: Hiernach bezeichnet Interoperabilität „*die Funktion eines Systems, Daten mit anderen Systemen unterschiedlichen Typs und/oder von unterschiedlichen Herstellern auszutauschen*“ (in [TR50572]).

Interoperabilität in dieser Definition darf deshalb nicht mit **Austauschbarkeit** verwechselt werden, welche als „*die Fähigkeit eines Produkts, Prozesses oder Dienstes anstelle eines Anderen genutzt zu werden, um dieselben Anforderungen zu erfüllen*“ (in [ISO/IEC-Voc]) bezeichnet wird.

Diese TR beinhaltet Mindestanforderungen an die Kommunikationseinheit eines intelligenten Messsystems, welche zwingend für eine Interoperabilität vorausgesetzt werden sowie darüberhinausgehende optionale Anforderungen. Diese sind jeweils entsprechend gekennzeichnet (▶Abschnitt 1.6).

2.3.2. Adaption des Interoperability Context-Setting Framework

Das folgende Interoperabilitätsmodell basiert auf dem „GridWise® Interoperability Context-Setting Framework“ (ICSF) des GridWise Architecture Council ([ICSF]). Das ICSF stellt einen Rahmen bereit, in dem die Interoperabilität komplexer Systeme systematisch betrachtet und vertieft werden kann.

Hierzu werden verschiedene Interoperabilitätskategorien und Querschnittsthemen identifiziert und gegenübergestellt. Diese grundsätzliche Herangehensweise des ICSF ist ebenfalls für die durch diese TR erfassten Smart-Meter-Gateways anwendbar; in der Detailbetrachtung ergeben sich jedoch einige Unterschiede, die im Folgenden dargestellt werden.

2.3.2.1. Erste Dimension: Interoperabilitätskategorien

Das ICSF differenziert den Begriff Interoperabilität und unterteilt diesen in unterschiedliche Ebenen:

Pragmatische Schicht Diese Schicht umfasst die Interoperabilität auf regulatorischen Ebene, d.h. die Kommunikationspartner müssen dieselben Richtlinien und Regeln einhalten, um auf pragmatischer Ebene miteinander kommunizieren zu können.

Interpretation im SMGW-Modell:

Im SMGW-Interoperabilitätsmodell besteht diese Schicht aus den gesetzlichen Anforderungen aus dem Messstellenbetriebsgesetz [MsbG] sowie dem Mess- und Eichgesetz mit zugehöriger Verordnung.

Semantische Schicht Diese Schicht umfasst die Interoperabilität auf semantischer Ebene. Hier werden die inhaltlichen Aspekte der Schnittstelle betrachtet, die meist über ein abgestimmtes Datenaustauschformat realisiert werden. D.h. in dieser Schicht wird die Frage geklärt, ob die Kommunikationspartner unter den übertragenen Daten im Kontext der pragmatischen Ebene dasselbe verstehen.

Interpretation im SMGW-Modell:

Im SMGW-Interoperabilitätsmodell besteht diese Schicht aus den verschiedenen Anwendungsfällen sowie den Kommunikationsszenarien.

Syntaktische Schicht Diese Schicht umfasst die Interoperabilität auf syntaktischer Ebene. Hier werden die strukturellen und ablaufspezifischen Aspekte der Schnittstelle betrachtet, die zwischen den Parteien in beiderseitig verständlichen Formaten ausgetauscht werden, wie z.B. Datentypen-Definitionen und übereinstimmende Implementierungen des Kommunikationsprotokolls. D.h. in dieser Schicht wird die Frage geklärt, ob die Kommunikationspartner die Daten in derselben Art und Weise übertragen.

Interpretation im SMGW-Modell:

Im SMGW-Interoperabilitätsmodell besteht diese Schicht aus den Datenmodellen, den zu verwendenden Protokollen, und der zugrundeliegenden physischen Schicht.

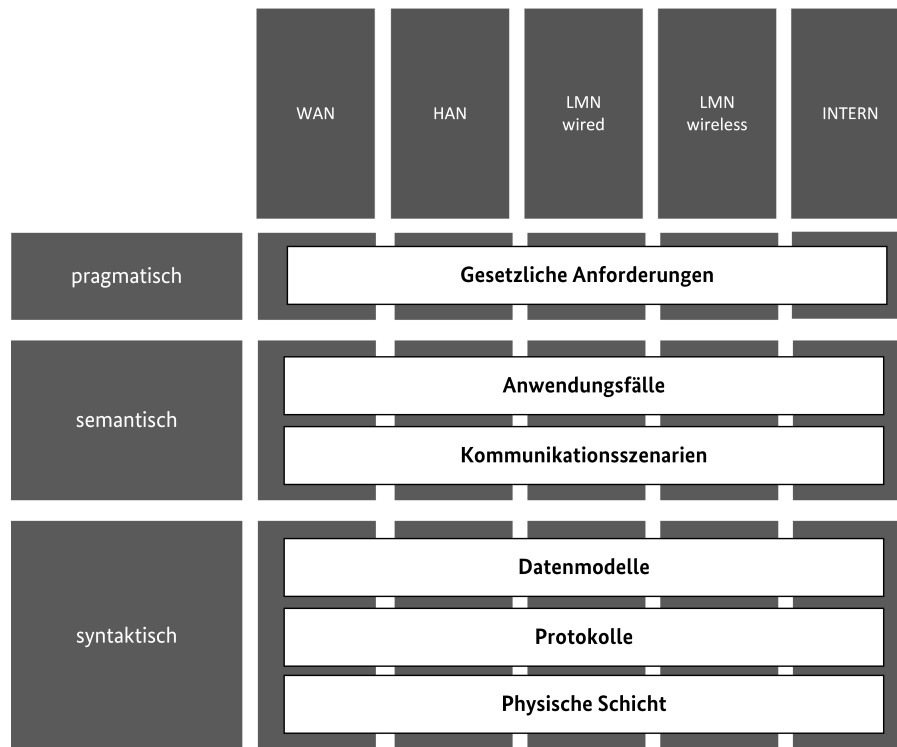


Abbildung 2.2. Interoperabilitätsmodell für SMGW

2.3.2.2. Zweite Dimension: Querschnittsthemen

Neben diesen verschiedenen Schichten werden – analog zum ICSF – Querschnittsthemen definiert, die die beschriebenen Schichten durchdringen. Diese bestehen aus thematischen Oberbegriffen und leiten sich direkt aus den Anforderungen an die Funktionalität eines SMGW (und damit größtenteils aus dem MsbG) ab.

In dieser TR sind für SMGW die funktionalen Anforderungen nach den jeweiligen Schnittstellen untergliedert – daher sind für diese Geräte als Querschnittsthemen die jeweiligen Schnittstellen (LMN, HAN, WAN) bzw. INTERN (für interne Prozesse und Dienste) vorgesehen.

Werden die Interoperabilitätskategorien auf der x-Achse und die Querschnittsthemen auf der y-Achse aufgetragen, ergibt sich eine Matrix, deren Eintragsfelder die jeweiligen definierten Teilziele („Feldziele“) für den Schnittpunkt zwischen Interoperabilitätskategorie und Querschnittsthema enthalten (so enthält z.B. der Schnittpunkt „semantisch / LMN-wired“ genau die Anwendungsfälle LAF 1 und LAF 2 sowie die Kommunikationsszenarien LKS 1 und LKS 2).

Auf diese Weise lässt sich ein Mapping der funktionalen Anforderungen dieser TR auf o.g. Matrix durchführen. Anschließend lässt sich für alle Teilziele prüfen, ob diese interoperabel umgesetzt sind. Grundsätzlich ist auch eine Interoperabilität nur auf einer Ebene (z. B. der pragmatischen) möglich.

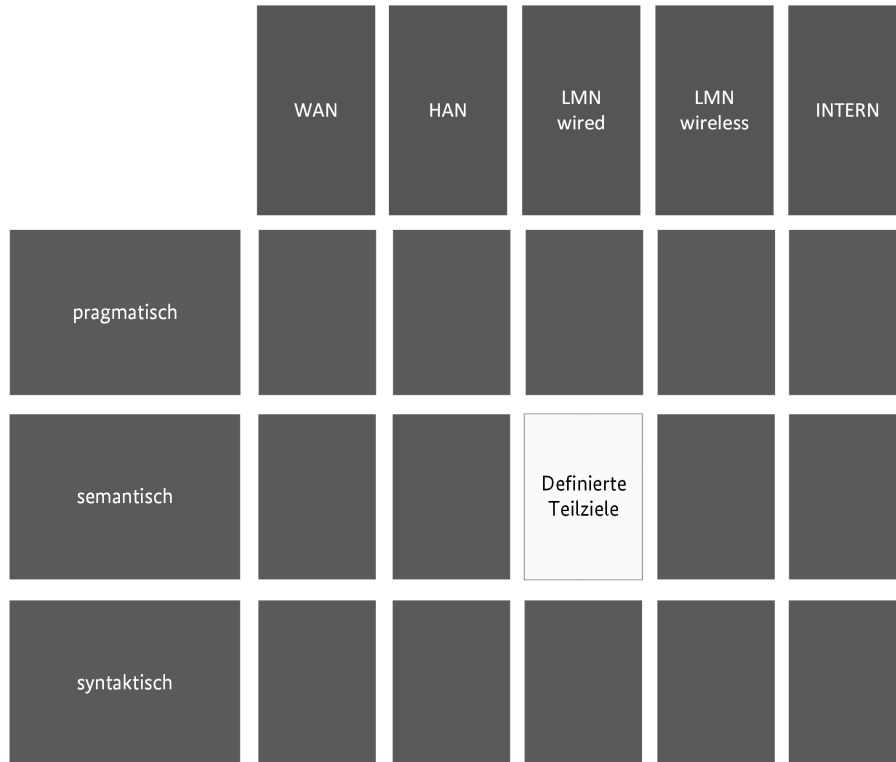


Abbildung 2.3. Die zwei Dimensionen des Interoperabilitätsmodells

2.3.3. Einordnung der Anforderungen ins Interoperabilitätsmodell

Die folgende Tabelle wendet das SMGW-Interoperabilitätsmodell auf die Anforderungen dieser TR an. Informativ Kapitel wurden dabei von der Betrachtung ausgenommen. Die in den Tabellenzellen stehenden Anforderungen definieren die auf das SMGW-Interoperabilitätsmodell projizierten normativen Anforderungen aus der TR als ideale Teilziele im Sinne der Interoperabilität.

	WAN	HAN	LMN-wired	LMN-wireless	INTERN
pragmatisch	Gesetzliche Anforderungen nach § 21 und 22 MsbG Insbesondere: Sichere Kommunikation durch Verschlüsselung und Signierung, Zeitsynchronisation, SM-PKI, Pseudonymisierung, Messwerterfassung/-verarbeitung/-versand, Softwareupdates				
semantisch	WAF WKS	HAF HKS		LAF LKS	TAF
syntaktisch	Physische Schnittstellen und Protokollspezifikationen (Detailspezifikationen)				/

Tabelle 2.1 Mapping der Anforderungen der TR auf das SMGW-Interoperabilitätsmodell

3. Anforderungen an die Kommunikationsverbindungen und Protokolle des SMGW

3.1. Einleitung

Das SMGW verfügt über Schnittstellen zum WAN, HAN und LMN (s. ▶Abbildung 2.1), um mit unterschiedlichen Marktteilnehmern und Komponenten in diesen Netzen zu kommunizieren.

Die folgenden Kapitel legen die Anforderungen an die Kommunikation über diese Schnittstellen im WAN (s. ▶Abschnitt 3.2), LMN (s. ▶Abschnitt 3.3) und HAN (s. ▶Abschnitt 3.4) fest.

3.2. Vorgaben an die Kommunikationsverbindungen im WAN

3.2.1. Übersicht

Anwendungsfälle, die eine WAN-Kommunikation erfordern, werden in ▶Abschnitt 3.2.2 kurz skizziert. Zur Realisierung dieser Anwendungsfälle werden mehrere Kommunikationsszenarien herangezogen, die die Komposition der Protokolle bei der Kommunikation mit einem Kommunikationspartner beschreiben. Die Kommunikationsszenarien werden in ▶Abschnitt 3.2.3 definiert.

Die Definition der Anforderungen an die Umsetzung der Kommunikationsprotokolle im WAN erfolgt in ▶Abschnitt 3.2.6.

Anforderungen an die Sicherung der Kommunikationsverbindungen im WAN werden in ▶Abschnitt 3.2.4 beschrieben.

Die Parametrierung der Kommunikationsverbindungen wird durch den GWA über Kommunikationsprofile durchgeführt, die in ▶Abschnitt 3.2.5 beschrieben sind.

Das funktionale Verhalten des SMGW bei der Führung der Systemzeit, der Netzwerkd Diagnose und den Selbsttests wird in den ▶Abschnitt 3.2.7, ▶Abschnitt 3.2.8 und ▶Abschnitt 3.2.9 beschrieben.

3.2.2. Anwendungsfälle an der WAN-Schnittstelle

Dieser Abschnitt listet diejenigen Anwendungsfälle auf (gekennzeichnet mit dem Kürzel WAF), die zwingend eine Kommunikation des SMGW mit Teilnehmern im WAN erfordern. Das SMGW **KANN** weitere Anwendungsfälle an der WAN-Schnittstelle unterstützen. [REQ.WAN.Anwendungsfaelle.10]

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

1. Administration und Konfiguration des SMGW durch den GWA
2. Zugriff des SMGW auf Dienste des GWA
 - a. Firmware-Download
 - b. Zeitsynchronisation
 - c. Weiterleitung von Nachrichten
3. Alarmierung und Benachrichtigung des GWA durch das SMGW

4. Übertragung von Daten des SMGW an EMT
5. Kommunikation von EMT mit einem CLS über das SMGW
6. Anforderung einer Management-Verbindung durch den GWA

3.2.2.1. WAF1: Administration und Konfiguration

Den Anwendungsfällen WAF1 ist gemein, dass der GWA einen vom SMGW bereitzustellenden Dienst aufruft, das SMGW den angeforderten Anwendungsfall ausführt und eine entsprechende Antwort (bei erfolgreicher Ausführung oder auch im Fehlerfall) an den GWA zurückliefert.

Das SMGW ermöglicht dem GWA mindestens die Realisierung der folgenden Anwendungsfälle:

- Geräteverwaltung - Anbindung einer Messeinrichtung
 - Das SMGW **MUSS** dem GWA das Anlegen und Aktualisieren der Parametrierung zum Herstellen der initialen kommunikativen Anbindung einer Messeinrichtung anbieten. [REQ.WAN.Management.10]
 - Das SMGW **MUSS** dem GWA das Löschen der Parametrierung für die kommunikative Anbindung einer Messeinrichtung anbieten. [REQ.WAN.Management.20]
 - Das SMGW **MUSS** dem GWA das Abfragen des Status der kommunikativen Anbindung einer Messeinrichtung anbieten. [REQ.WAN.Management.30]
- Geräteverwaltung - Anbindung von HAN-Komponenten
 - Das SMGW **MUSS** dem GWA das Anlegen und Aktualisieren der Parametrierung von Profilen zum Herstellen der kommunikativen Anbindung von HAN-Komponenten des Anschlussnutzers oder Service-Technikers anbieten. [REQ.WAN.Management.40]¹
 - Das SMGW **MUSS** dem GWA das Löschen der Parametrierung von Profilen zum Herstellen der kommunikativen Anbindung von HAN-Komponenten des Anschlussnutzers oder Service-Technikers anbieten. [REQ.WAN.Management.50]
- Anschlussnutzerverwaltung
 - Das SMGW **MUSS** dem GWA das Anlegen und Aktualisieren der Parametrierung eines Anschlussnutzer-Kontos anbieten. [REQ.WAN.Management.60]
 - Das SMGW **MUSS** dem GWA das Löschen der Parametrierung eines Anschlussnutzer-Kontos anbieten. [REQ.WAN.Management.70]
- CLS-Proxy Verwaltung
 - Das SMGW **MUSS** dem GWA das Anlegen und Aktualisieren von Profilen zur Vermittlung von Proxy-Kommunikationsverbindungen zwischen CLS und aktivem EMT anbieten. [REQ.WAN.Management.80]
 - Das SMGW **MUSS** dem GWA das Löschen von Profilen zur Vermittlung von Proxy-Kommunikationsverbindungen zwischen CLS und aktivem EMT anbieten. [REQ.WAN.Management.90]
 - Das SMGW **MUSS** dem GWA das Initiieren einer Proxy-Kommunikationsverbindung zwischen aktivem EMT und CLS anbieten. [REQ.WAN.Management.100]
 - Das SMGW **MUSS** dem GWA das Beenden einer Proxy-Kommunikationsverbindung zwischen aktivem EMT und CLS anbieten. [REQ.WAN.Management.110]
- Auswertungsprofile

¹ Die Anzeigeeinheit des Anschlussnutzers kann beispielsweise ein Gerät mit einer Transparenz- und Display-Software ("Sichtanzeige nach [MessEG]/[MessEV]") zur lokalen Rechnungsprüfung oder ein Display zur Anzeige von Energieverbrauchsinformationen sein.

- Das SMGW **MUSS** dem GWA das Anlegen eines Auswertungsprofils anbieten. [REQ.WAN.Management.120]
- Das SMGW **MUSS** dem GWA das Löschen eines Auswertungsprofils anbieten. [REQ.WAN.Management.130]
- Das SMGW **MUSS** dem GWA das Einspielen eines WAN-Kommunikationsprofils und der Zertifikate zum kommunikativen Anbinden eines EMT als Messwertempfänger anbieten. [REQ.WAN.Management.140]
- Das SMGW **MUSS** dem GWA das Löschen des WAN-Kommunikationsprofils und der Zertifikate zur kommunikativen Anbindung eines EMT als Messwertempfänger anbieten. [REQ.WAN.Management.150]
- Schlüssel-/Zertifikatsmanagement
 - Das SMGW **MUSS** dem GWA die Authentifizierung am Sicherheitsmodul anbieten, damit er dieses verwalten kann. [REQ.WAN.Management.160]
 - Das SMGW **MUSS** dem GWA die Verwaltung der zur Kommunikation im WAN, HAN und LMN verwendeten Schlüssel und Schlüsselpaare anbieten. [REQ.WAN.Management.170]
 - Das SMGW **MUSS** dem GWA das Importieren von RootCA-Zertifikaten der SM-PKI anbieten. [REQ.WAN.Management.180]
 - Das SMGW **SOLL** dem GWA das Löschen von RootCA-Zertifikaten der SM-PKI anbieten. [REQ.WAN.Management.181]
 - Das SMGW **MUSS** dem GWA das Aktualisieren seiner GWA-Zertifikate, der EMT-Zertifikate und der SubCA-Zertifikate anbieten. [REQ.WAN.Management.190]
 - Das SMGW **MUSS** dem GWA das Erzeugen von Zertifikats-Requests und die Aktualisierung der SMGW-WAN-Zertifikate anbieten. [REQ.WAN.Management.200]
 - Das SMGW **MUSS** dem GWA die Aktualisierung der SMGW-LMN-Zertifikate und der im SMGW hinterlegten, zählerindividuellen Schlüssel MK anbieten. [REQ.WAN.Management.210]
 - Das SMGW **MUSS** dem GWA das Aktualisieren der SMGW-HAN-Zertifikate anbieten. [REQ.WAN.Management.220]
 - Das SMGW **MUSS** dem GWA den Wechsel der Parametrierung der kommunikativen Anbindung vom bisherigen zum künftigen GWA anbieten. [REQ.WAN.Management.230]
- Firmware-Update
 - Das SMGW **MUSS** dem GWA das Übertragen und Aktivieren einer erfolgreich validierten Firmware auf das SMGW anbieten. [REQ.WAN.Management.240] Dies kann entweder durch einen Upload durch den GWA erfolgen oder durch einen Dienst im SMGW über den der GWA einen Download der Firmware durch das SMGW initiiert wird.
 - Falls die übertragene, validierte Firmware nicht durch das SMGW nach der Übertragung aktiviert wird, **MUSS** das SMGW dem GWA anbieten, die Aktivierung einer neuen Firmware des GWA auszulösen. [REQ.WAN.Management.250]
- Wake-Up-Konfiguration

Das SMGW **KANN** dem GWA die Konfiguration der Wake-Up-Adresse (z.B. UDP-Port) für die Anforderung einer Management-Kommunikationsverbindung anbieten. [REQ.WAN.Management.260]²
- Zeitsynchronisation

² Die Formulierung ist bewusst technologie-neutral gewählt; dies kann beispielsweise ein UDP-Port des SMGW oder Mobile-Messaging-Parameter sein.

Das SMGW **MUSS** dem GWA die Konfiguration der Parameter zur zuverlässigen Durchführung der Synchronisation mit dem Zeitserver des GWA anbieten. [REQ.WAN.Management.270]

- SMGW-Monitoring
 - Das SMGW **MUSS** dem GWA das Exportieren der System-Logbucheinträge anbieten. [REQ.WAN.Management.280]
 - Das SMGW **MUSS** dem GWA das Exportieren der durch das SMGW signierten Eichlog-Einträge für Tätigkeiten gemäß [MessEG]/[MessEV] berechtigter Stellen anbieten. [REQ.WAN.Management.290]
 - Falls das SMGW einen Netzwerkdiagnoseservice gemäß ▶ICS.NDS.Umsetzung.10 anbietet, **MUSS** das SMGW dem GWA das Anlegen, Aktualisieren und Löschen der Konfigurationsprofile für die Netzwerkschnittstellen-Diagnose anbieten. [REQ.WAN.Management.300]

- Selbsttest

Das SMGW **MUSS** dem GWA das Auslösen von Selbsttests des SMGW anbieten. [REQ.WAN.Management.310]



ICS.WAN.WakeUpKonfiguration.10

Der GWH **MUSS** im ICS deklarieren, ob der GWA die Wake-Up-Adresse (z.B. UDP-Port) des SMGW konfigurieren kann.



ICS.WAN.RootCAZertifikatLoeschen.10

Der GWH **MUSS** im ICS deklarieren, ob der GWA ein RootCA-Zertifikat im SMGW löschen kann.

3.2.2.2. WAF2: Zugriff auf Dienste beim GWA

Die folgenden Dienste, auf die das SMGW im Betrieb angewiesen ist, werden vom GWA bereitgestellt:

- Zeitsynchronisation

Das SMGW **MUSS** seine Systemzeit mit einem vertrauenswürdigen Zeitdienst beim GWA synchronisieren können. [REQ.WAN.ZugriffAufGwaDienste.10]

- Firmware-Download

Das SMGW **MUSS** einen Dienst beim GWA nutzen können, um neue Firmware herunterzuladen. [REQ.WAN.ZugriffAufGwaDienste.20]

- Auslieferung von tarifierten Messwerten zur Weiterleitung an EMT

Das SMGW **SOLL** gemäß der durch den GWA parametrisierten Auswerte- und Kommunikationsprofile, die für einen EMT verschlüsselten, tarifierten Messwerte, turnusmäßig oder im Bedarfsfall an den GWA ausliefern können. [REQ.WAN.ZugriffAufGwaDienste.30] Der GWA leitet die verschlüsselte Nachricht dann an den EMT weiter.

- Auslieferung von pseudonymisierte Messwerten (Netzzustandsdaten) zur Weiterleitung an EMT

Das SMGW **SOLL** gemäß der durch den GWA parametrisierten Auswerte- und Kommunikationsprofile, die für einen EMT verschlüsselten, pseudonymisierten Messwerte (Netzzustandsdaten) an den GWA ausliefern können. [REQ.WAN.ZugriffAufGwaDienste.40] Der GWA entfernt die äußere Signatur des SMGW und leitet die verschlüsselte Nachricht dann an den EMT weiter.

- Übermittlung von Diagnosedaten der Netzwerkschnittstelle

Falls das SMGW einen Netzwerkdiagnoseservice gemäß ▶ICS.NDS.Umsetzung.10 umsetzt, **MUSS** das SMGW einen Dienst beim GWA nutzen können, um Netzwerkdiagnosedaten an den GWA zu übertragen. [REQ.WAN.ZugriffAufGwaDienste.50]



ICS.WAN.ZugriffAufGwaDienste.10

Der GWH **MUSS** im ICS deklarieren, ob das SMGW über den GWA für den EMT verschlüsselte, tarifizierte Messwerte ausliefern kann.



ICS.WAN.ZugriffAufGwaDienste.20

Der GWH **MUSS** im ICS deklarieren, ob das SMGW über den GWA für den EMT verschlüsselte, pseudonymisierte Messwerte (Netzzustandsdaten) ausliefern kann.

3.2.2.3. WAF3: Alarmierung und Benachrichtigung

Das SMGW **MUSS** während des Betriebs auftretende Ereignisse oder Fehlersituationen an den GWA melden. [REQ.WAN.GwaBenachrichtigung.10]

3.2.2.4. WAF4: Übertragung von Daten an den GWA

Dieser Anwendungsfall entfällt, da er Bestandteil des WAF2 ist.

3.2.2.5. WAF5: Übertragung von Daten an EMT

Das SMGW übergibt die Daten an eine Dienstschnittstelle beim EMT, die die sichere und interoperable Auslieferung durch das SMGW ermöglicht.

Bei der Übertragung von Daten des SMGW an einen EMT treten folgende Anwendungsfälle auf:

- Turnusmäßige Auslieferung von tarifizierten Messwerten

Das SMGW **MUSS** gemäß einem Auswertungsprofil und einem WAN-Kommunikationsprofils regelmäßig *abrechnungsrelevante Messwerte* zur Tarifizierung für einen EMT ausliefern können. [REQ.WAN.EmtBenachrichtigung.10]

- Turnusmäßige Netzzustandsdatenauslieferung

Das SMGW **MUSS** gemäß einem Auswertungsprofil und einem WAN-Kommunikationsprofil regelmäßig Messwerte zum Netzzustand für einen EMT ausliefern können. [REQ.WAN.EmtBenachrichtigung.20]

- Spontane Messwertauslesung

Ein EMT hat keinen direkten Zugriff auf die Daten des SMGW. Daher **MUSS** das SMGW dem GWA einen Dienst anbieten, mit dem der GWA ein geeignetes Auswertungs- und WAN-Kommunikationsprofil in das SMGW einbringt (falls noch nicht vorhanden), das die Auslieferung der benötigten Messwerte an den EMT auslöst. [REQ.WAN.EmtBenachrichtigung.30]

Das anschließende WAN-Kommunikationsverhalten entspricht dann einer Weitergabe von Messwerten wie bei einer turnusmäßigen Auslieferung.

- Übermittlung von Diagnosedaten der Netzwerkschnittstelle

Falls das SMGW einen Netzwerkdiagnoseservice gemäß ▶ICS.NDS.Umsetzung.10 umsetzt, **MUSS** das SMGW gemäß eines Konfigurationsprofils ereignisgesteuert Informationen zur Diagnose der Qualität der kommunikativen Netzwerkanbindung ausliefern können. [REQ.WAN.EmtBenachrichtigung.40]

3.2.2.6. WAF6: Kommunikation aktiver EMT mit CLS

Das SMGW **MUSS** Anwendungsfälle zur Kommunikation eines aktiven EMT mit einem CLS-Gerät unter Nutzung der Proxy-Funktionalität des SMGW unterstützen. [REQ.WAN.TlsProxy.10]

3.2.2.7. WAF7: Anforderung einer Management-Verbindung (Wake-Up-Service)

Das SMGW **MUSS** dem GWA über den Wake-Up-Service gemäß ▶Abschnitt 3.2.6.3 ermöglichen, eine "MANAGEMENT"-Verbindung (siehe ▶Abschnitt 3.2.3.1) zur Realisierung des WAF1 anzufordern. [REQ.WAN.WakeUp.10]



ICS.WAN.WakeUp.10

Der GWH **MUSS** im ICS deklarieren, ob die Wake-Up-Adresse geändert werden kann.



ICS.WAN.Anwendungsfaelle.10

Der GWH **MUSS** im ICS deklarieren, ob über WAF1 bis WAF7 hinausgehend weitere WAN Anwendungsfälle unterstützt werden. Sofern dies der Fall ist beschreibt er diese in einer Anlage zum ICS.

3.2.3. Kommunikationsszenarien

Die in ▶Abschnitt 3.2.2 skizzierten Anwendungsfälle an der WAN-Schnittstelle lassen sich auf folgende Kommunikationsszenarien (gekennzeichnet mit dem Kürzel WKS) abbilden.

- MANAGEMENT (Administration)
Zugriff des GWA auf Services des SMGW, die das SMGW an seiner WAN-Schnittstelle dem GWA anbietet.
Siehe ▶Abschnitt 3.2.3.1.
- ADMIN-SERVICE
Zugriff des SMGW auf Services des GWA, die dieser an seiner WAN-Schnittstelle dem SMGW anbietet.
Siehe ▶Abschnitt 3.2.3.2.
- INFO-REPORT
Zugriff des SMGW auf Services des EMT zum Versand von Daten durch das SMGW an den EMT.
Siehe ▶Abschnitt 3.2.3.3.
- NTP-HTTPS
Zeitsynchronisierung über einen vom GWA bereitgestellten Webservice.
Siehe ▶Abschnitt 3.2.3.4.
- NTP-TLS
Zeitsynchronisierung über einen vom GWA bereitgestellten NTP-Service.
Siehe ▶Abschnitt 3.2.3.5.
- TLSPROXY
TLS-Kommunikationsverbindung vom SMGW zum aktiven EMT.
Siehe ▶Abschnitt 3.2.3.6.
- WAKEUP
Anfordern einer MANAGEMENT-Verbindung durch den GWA.
Siehe ▶Abschnitt 3.2.3.7.

Das SMGW **MUSS** die WAN Kommunikationsszenarien MANAGEMENT, ADMIN-SERVICE, INFO-REPORT, TLSPROXY und WAKEUP umsetzen. [REQ.WAN.Kommunikationsszenarien.10]

Das SMGW **MUSS** mindestens eines der beiden Kommunikationsszenarien NTP-TLS oder NTP-HTTPS umsetzen. [REQ.WAN.Kommunikationsszenarien.20] NTP-HTTPS wird nicht für Neuentwicklungen empfohlen.

Ein Kommunikationsszenario definiert die technischen Rollen der SMGW und seines Kommunikationspartners für jede Schicht des Protokollstapels. ▶Tabelle 3.1 enthält eine Übersicht dieser Rollen je Kommunikationsszenario.

Szenario	Typ	TLS-Server	Webservice-Server	Inhaltsdaten-Empfänger	Inhaltsdaten-Ab-sender
WKS1	MANAGEMENT	GWA	SMGW	GWA, SMGW	GWA, SMGW
WKS2	ADMIN-SERVICE	GWA	GWA	GWA, SMGW	GWA, SMGW
WKS3	INFO-REPORT	EMT	EMT	EMT	SMGW
WKS4	NTP-HTTPS	GWA	GWA	-	-
WKS5	NTP-TLS	GWA	-	-	-
WKS6	TLSPROXY	aEMT	-	-	-
WKS7	WAKEUP	-	-	SMGW	GWA

Tabelle 3.1 Kommunikationsszenarien an der WAN-Schnittstelle

Innerhalb einer TLS-Verbindung des SMGW **MUSS** genau ein Kommunikationsszenario ablaufen. [REQ.WAN.Kommunikationsszenarien.30] Ein Wechsel des Kommunikationsszenarios während einer bestehenden TLS-Verbindung **DARF NICHT** vorgenommen werden. [REQ.WAN.Kommunikationsszenarien.40] Das SMGW **MUSS** mindestens so viele gleichzeitige TLS-Verbindungen zum GWA und zum EMT unterhalten können, dass die Ausführung je eines Anwendungsfalles aus WAF1-WAF6 ohne Blockieren eines Anwendungsfalles aus einem anderen WAF1-WAF6 gewährleistet ist. [REQ.WAN.Kommunikationsszenarien.50]

3.2.3.1. MANAGEMENT

Das folgende Diagramm zeigt das Kommunikationsmuster des „MANAGEMENT“ Szenarios.

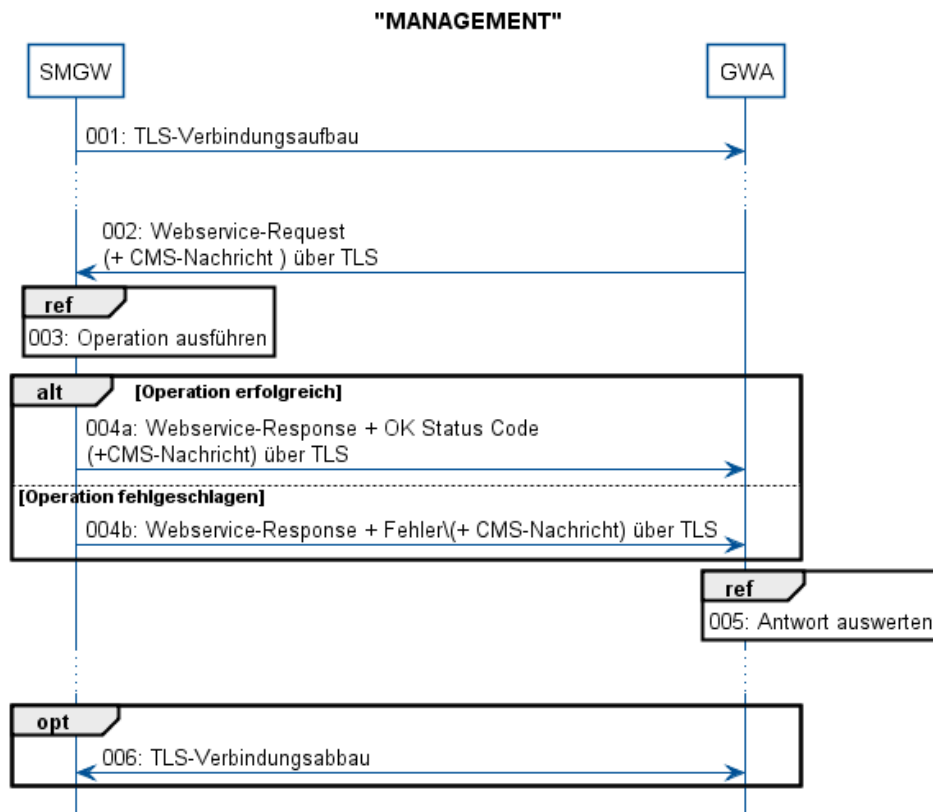


Abbildung 3.1. Sequenzdiagramm Kommunikationsszenario „MANAGEMENT“

Vorbedingung:

Die Kommunikationsadresse zum Zugriff auf Management-Services beim SMGW ist dem GWA bekannt.

Rolle des SMGW:

TLS-Client, Webservice-Server, CMS-Originator, CMS-Recipient

Schritt	Ereignis	Aktivität	Sender oder Initiator	Empfänger	Ausgetauschte Daten
001	TLS-Verbindung für "MANAGEMENT" besteht nicht	TLS-Verbindungs-aufbau zum GWA	SMGW	GWA	Informationen zum TLS-Verbindungs-aufbau
002	Dienstaufruf des SMGW initiiert	GWA erstellt und sendet Webservice-Request	GWA	SMGW	Webservice-Request (+CMS-Daten)
003	SMGW empfängt Webservice-Request	SMGW führt Operation aus	-	-	-
004a	Operation erfolgreich beendet	SMGW sendet Webservice-Response an GWA	SMGW	GWA	Webservice-Response-Code OK (+ CMS-Data)
004b	Operation nicht erfolgreich beendet	SMGW sendet Webservice-Response an GWA	SMGW	GWA	Webservice-Response mit Fehler Code (+ CMS-Data)
005	GWA empfängt Response	GWA verarbeitet Response	-	-	-

Schritt	Ereignis	Aktivität	Sender oder Initiator	Empfänger	Ausgetauschte Daten
006	SMGW oder GWA initiiert TLS-Verbindungsabbau	TLS-Verbindungsabbau	SMGW, GWA	GWA, SMGW	Informationen zum TLS-Verbindungsabbau

Tabelle 3.2 Beschreibung Kommunikationsszenario „MANAGEMENT“

Umzusetzende Anwendungsfälle:

Das SMGW **MUSS** zur Umsetzung des Anwendungsfalles WAF1 über das Kommunikationsszenario "MANAGEMENT" mit dem GWA kommunizieren. [REQ.WAN.Kommunikationsszenarien.60]

3.2.3.2. ADMIN-SERVICE

Das folgende Diagramm zeigt das Kommunikationsmuster des „ADMIN-SERVICE“ Szenarios.

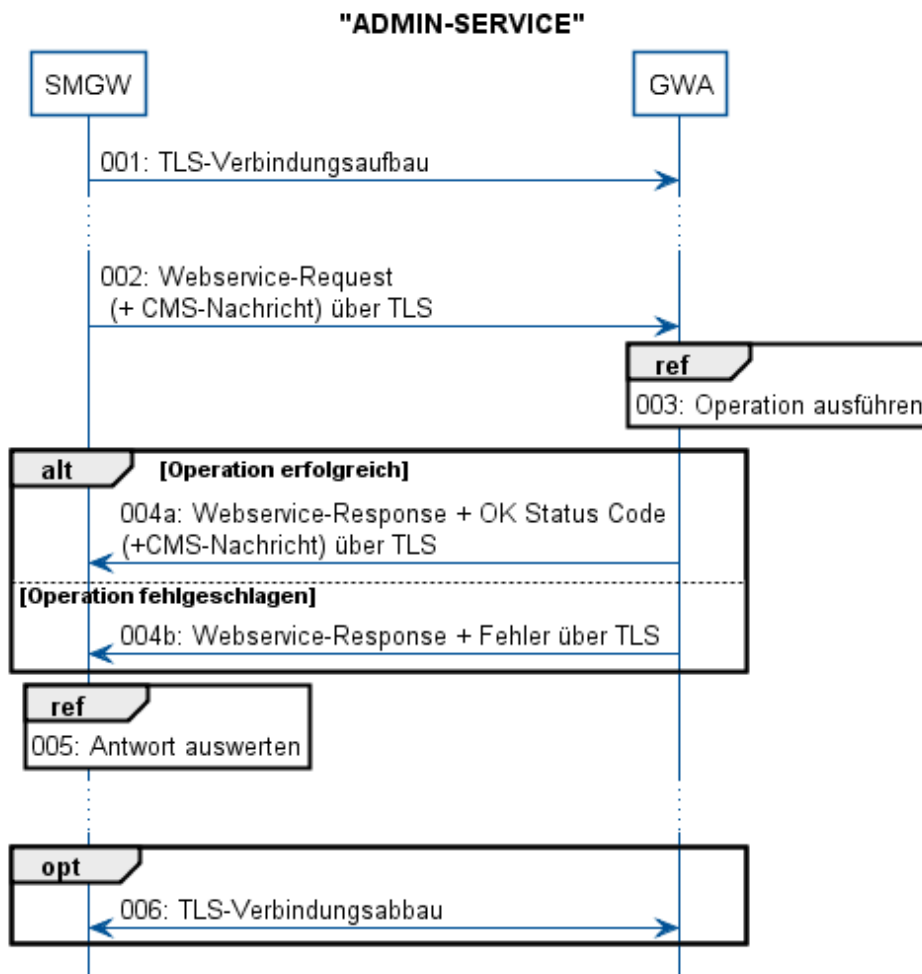


Abbildung 3.2. Sequenzdiagramm Kommunikationsszenario „ADMIN-SERVICE“

Vorbedingung:

Die Kommunikationsadresse zum Zugriff auf Admin-Services beim GWA ist dem SMGW bekannt.

Rolle des SMGW:

TLS-Client, Webservice-Client, CMS-Originator, CMS-Recipient. Zur Absicherung mit CMS für Firmware und Zeitsynchronisation siehe ▶Abschnitt 3.2.4.2.

Schritt	Ereignis	Aktivität	Sender oder Initiator	Empfänger	Ausgetauschte Daten
001	TLS-Verbindung für "ADMIN-SERVICE" besteht nicht	TLS-Verbindungsaufbau zum GWA	SMGW	GWA	Informationen zum TLS-Verbindungsaufbau
002	Dienstaufruf des GWA initiiert	SMGW sendet Webservice-Request	SMGW	GWA	Webservice-Request (+CMS-Data)
003	GWA empfängt Webservice-Request	GWA verarbeitet Webservice-Request	-	-	-
004a	Webservice-Request wurde erfolgreich vom GWA verarbeitet	GWA sendet Webservice-Response	GWA	SMGW	Webservice-Response-Code OK (+CMS-Data)
004b	Request wurde nicht erfolgreich vom GWA verarbeitet	GWA sendet Webservice-Response	GWA	SMGW	Webservice-Response mit Fehler Code (+ CMS-Data)
005	SMGW empfängt Webservice-Response	SMGW verarbeitet Response	-	-	-
006	SMGW oder GWA initiiert TLS-Verbindungsabbau	TLS-Verbindungsabbau	SMGW, GWA	GWA, SMGW	Informationen zum TLS-Verbindungsabbau

Tabelle 3.3 Beschreibung Kommunikationsszenario „ADMIN-SERVICE“

Umzusetzende Anwendungsfälle:

Das SMGW **MUSS** zur Umsetzung des Anwendungsfalles WAF2 - Firmware-Download und WAF3 über das Kommunikationsszenario "ADMIN-SERVICE" mit dem GWA kommunizieren. [REQ.WAN.Kommunikationsszenarien.70] Zur Absicherung mit CMS für Firmware und Zeitsynchronisation siehe ▶Abschnitt 3.2.4.2.

3.2.3.3. INFO-REPORT

Das folgende Diagramm zeigt das Kommunikationsmuster des „INFO-REPORT“ Szenarios.

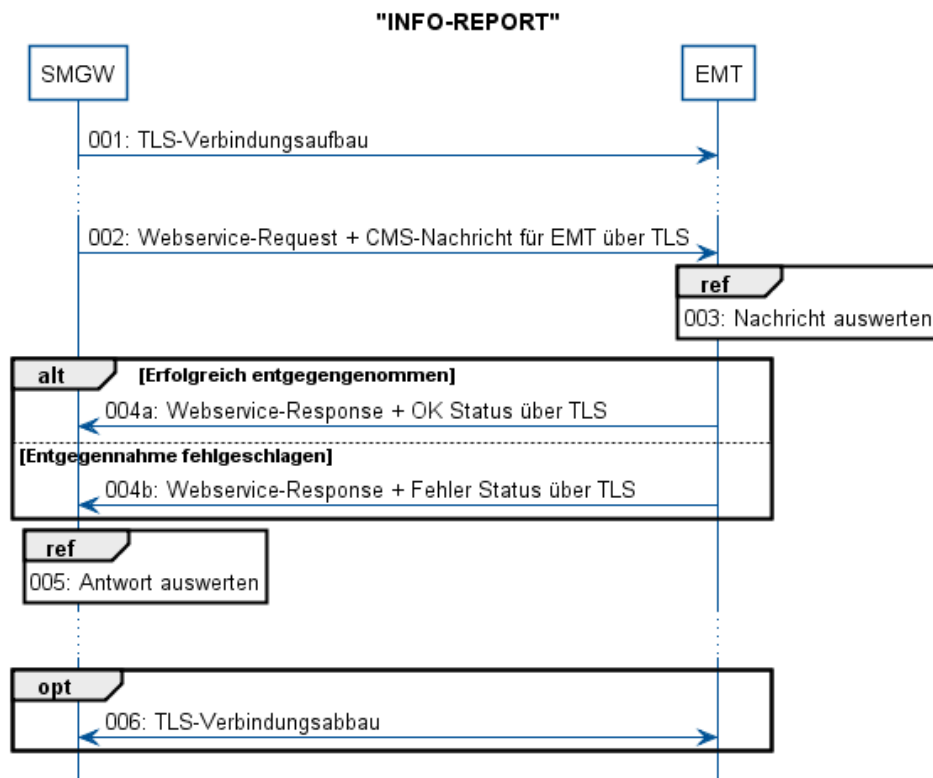


Abbildung 3.3. Sequenzdiagramm Kommunikationsszenario „INFO-REPORT“

Vorbedingung:

Die Kommunikationsadresse zum Zugriff auf Info-Report-Services beim EMT ist dem SMGW bekannt.

Rolle des SMGW:

TLS-Client, Webservice-Client, CMS-Originator

Schritt	Ereignis	Aktivität	Sender oder Initiator	Empfänger	Ausgetauschte Daten
001	TLS-Verbindung zum Nachrichtensend an EMT besteht nicht	TLS-Verbindungsaufbau zum EMT	SMGW	EMT	Informationen zum TLS-Verbindungsaufbau
002	-	SMGW sendet Webservice-Request	SMGW	EMT	Webservice-Request (+CMS-Data)
003	EMT empfängt Request	EMT verarbeitet Request-Daten			
004a	Webservice-Request wurde erfolgreich vom EMT verarbeitet	EMT sendet Webservice-Response	EMT	SMGW	Webservice-Response-Code OK
004b	Request wurde nicht erfolgreich vom EMT verarbeitet	EMT sendet Webservice-Response	EMT	SMGW	Webservice-Response mit Fehler Code

Schritt	Ereignis	Aktivität	Sender oder Initiator	Empfänger	Ausgetauschte Daten
005	SMGW empfängt Webservice-Response	SMGW verarbeitet Response	-	-	-
006	SMGW oder EMT initiiert TLS-Verbindungsabbau	TLS-Verbindungsabbau	SMGW, EMT	EMT, SMGW	Informationen zum TLS-Verbindungsabbau

Tabelle 3.4 Beschreibung Kommunikationsszenario „INFO-REPORT“

Umzusetzende Anwendungsfälle:

Das SMGW **MUSS** zur Umsetzung des Anwendungsfalles WAF5 über das Kommunikationsszenario "INFO-REPORT" mit dem EMT kommunizieren. [REQ.WAN.Kommunikationsszenarien.80]

3.2.3.4. NTP-HTTPS

Dieses Kommunikationsszenario entspricht WKS ADMIN-SERVICE, jedoch ohne CMS. Es wird für die Zeitsynchronisation über den ADMIN-SERVICE verwendet.

Das folgende Diagramm zeigt das Kommunikationsmuster des „NTP-HTTPS“ Szenarios.

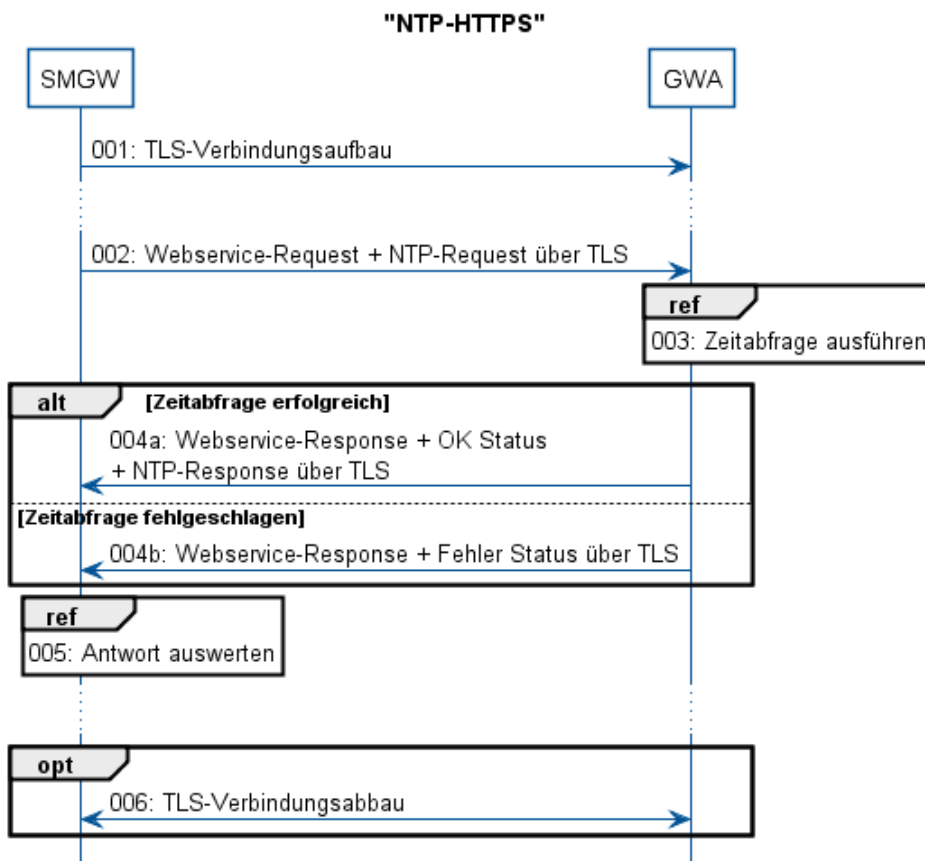


Abbildung 3.4. Sequenzdiagramm Kommunikationsszenario „NTP-HTTPS“

Vorbedingung:

Die Kommunikationsadresse zum Zugriff auf den Zeitserver beim GWA ist dem SMGW bekannt.

Rolle des SMGW:

TLS-Client, Webservice-Client

Schritt	Ereignis	Aktivität	Sender oder Initiator	Empfänger	Ausgetauschte Daten
001	TLS-Verbindung zur Zeitsynchronisation besteht nicht	TLS-Verbindungsaufbau zum GWA	SMGW	GWA	Informationen zum TLS-Verbindungsaufbau
002	Initiieren der Zeitsynchronisation	SMGW sendet Webservice-Request	SMGW	GWA	Webservice-Request mit NTP-Request
003	GWA empfängt Webservice-Request	GWA verarbeitet NTP Paket aus Webservice-Request	-	-	-
004a	NTP Paket wurde erfolgreich vom GWA verarbeitet	GWA sendet Webservice-Response "OK"	GWA	SMGW	Webservice-Response mit NTP-Response
004b	NTP Paket wurde nicht erfolgreich vom GWA verarbeitet	GWA sendet Webservice-Response "Fehler"	GWA	SMGW	Webservice-Response
005	SMGW empfängt Webservice-Response	Falls Webservice-Response "OK" verarbeitet das SMGW das NTP Paket	-	-	-
006	SMGW oder GWA initiiert TLS-Verbindungsabbau	TLS-Verbindungsabbau	SMGW, GWA	GWA, SMGW	Informationen zum TLS-Verbindungsabbau

Tabelle 3.5 Beschreibung Kommunikationsszenario „NTP-HTTPS“

**ICS.WAN.Kommunikationsszenarien.10**

Der GWH **MUSS** im ICS deklarieren, ob das SMGW das Kommunikationsszenario NTP-HTTPS unterstützt.

3.2.3.5. NTP-TLS

Das folgende Diagramm zeigt das Kommunikationsmuster des „NTP-TLS“ Szenarios.

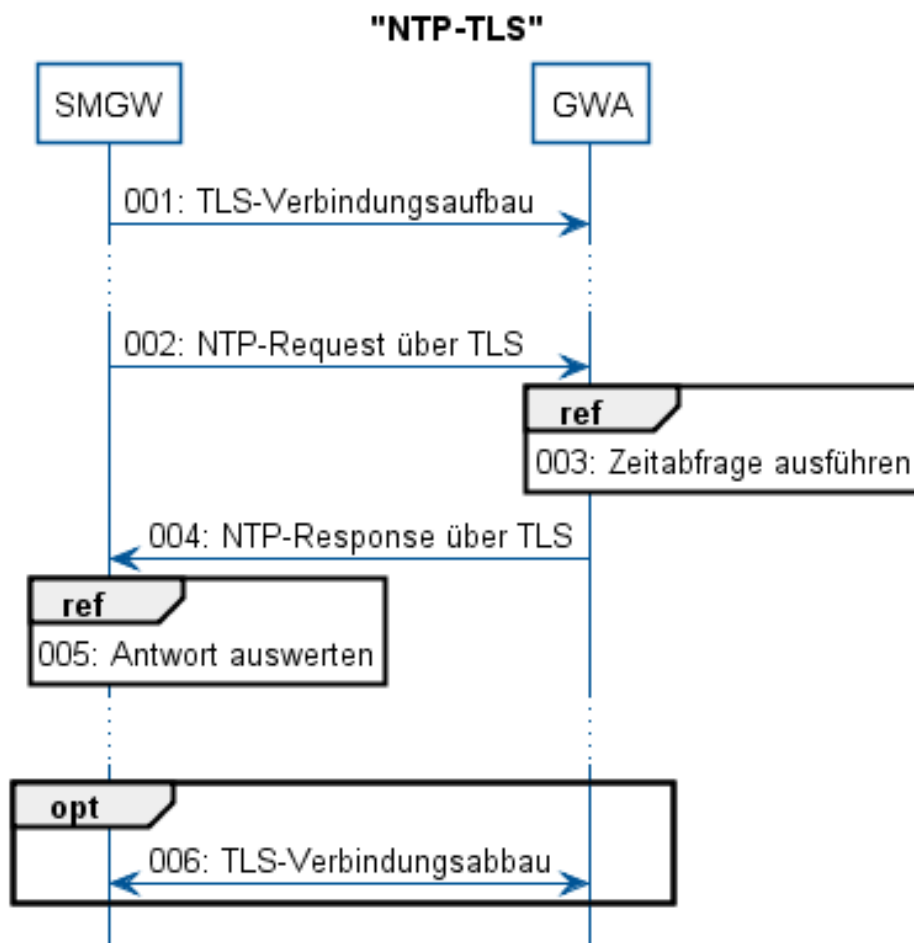


Abbildung 3.5. Sequenzdiagramm Kommunikationsszenario „NTP-TLS“

Vorbedingung:

Die Kommunikationsadresse zum Zugriff auf den Zeitserver beim GWA ist dem SMGW bekannt.

Rolle des SMGW:

TLS-Client

Schritt	Ereignis	Aktivität	Sender oder Initiator	Empfänger	Ausgetauschte Daten
001	TLS-Verbindung zur Zeitsynchronisation besteht nicht	TLS-Verbindungsaufbau zum GWA	SMGW	GWA	Informationen zum TLS-Verbindungsaufbau
002	Initiieren der Zeitsynchronisation	SMGW sendet NTP Paket	SMGW	GWA	NTP-Request
003	GWA empfängt NTP Paket	GWA führt Zeitabfrage durch	-	-	-
004	NTP Paket wurde erfolgreich vom GWA verarbeitet	GWA sendet NTP Paket	GWA	SMGW	NTP-Response
005	SMGW empfängt NTP Paket	SMGW verarbeitet NTP Paket	-	-	-

Schritt	Ereignis	Aktivität	Sender oder Initiator	Empfänger	Ausgetauschte Daten
006	SMGW oder GWA initiiert TLS-Verbindungsabbau	TLS-Verbindungsabbau	SMGW, GWA	GWA, SMGW	Informationen zum TLS-Verbindungsabbau

Tabelle 3.6 Beschreibung Kommunikationsszenario „NTP-TLS“

Umzusetzende Anwendungsfälle:

Das SMGW **MUSS** zur Umsetzung der Anwendungsfalles WAF2 - Zeitsynchronisation entweder über das Kommunikationsszenario "NTP-HTTPS" oder über das Kommunikationsszenario "NTP-TLS" mit dem Zeitserver des GWA kommunizieren. [REQ.WAN.Kommunikationsszenarien.90]



ICS.WAN.Kommunikationsszenarien.20

Der GWA **MUSS** im ICS deklarieren, ob das SMGW das Kommunikationsszenario NTP-TLS unterstützt.

3.2.3.6. TLSPROXY (WAN-seitig HKS3, HKS4, HKS5)

Das folgende Diagramm zeigt das Kommunikationsmuster des „TLSPROXY“ Szenarios.

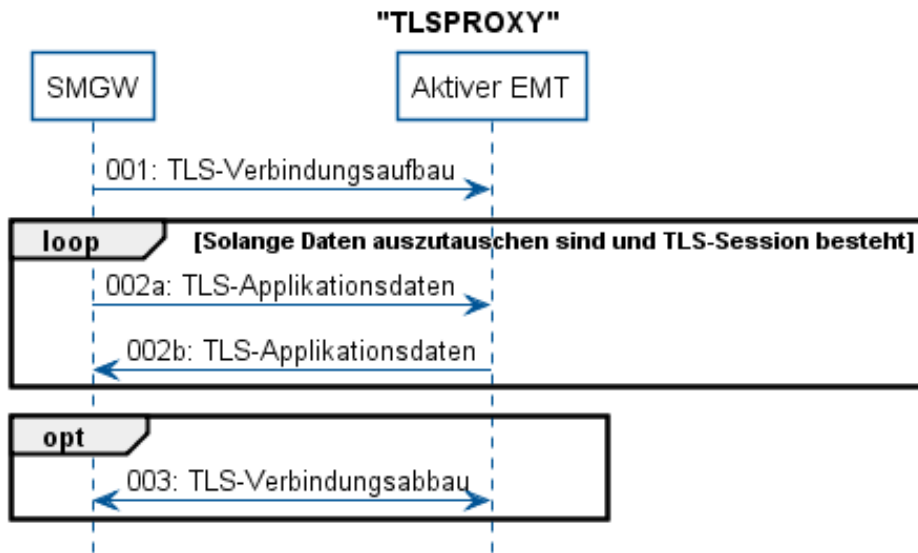


Abbildung 3.6. Sequenzdiagramm Kommunikationsszenario „TLSPROXY“

Die Ablaufschritte 002a und 002b können in beliebiger Reihenfolge, auch mehrmals auftreten.

Vorbedingung:

Die Kommunikationsadresse zum Zugriff auf den TLSPROXY-Service beim aktiven EMT ist dem SMGW bekannt.

Rolle des SMGW:

TLS-Client

Schritt	Ereignis	Aktivität	Sender oder Initiator	Empfänger	Ausgetauschte Daten
001	CLS oder SMGW initiiert TLS-Verbindungsaufbau	TLS-Verbindungsaufbau zum aEMT	SMGW	aEMT	Informationen zum TLS-Verbindungsaufbau

Schritt	Ereignis	Aktivität	Sender oder Initiator	Empfänger	Ausgetauschte Daten
002a	SMGW empfängt Daten vom CLS (über HKS3, HKS4, HKS5) bzw.	SMGW leitet Daten als Proxy weiter	SMGW	aEMT	Für das SMGW transparente Daten
002b	SMGW empfängt Daten vom aEMT	SMGW leitet Daten als Proxy weiter (über HKS3, HKS4, HKS5)	aEMT	SMGW	Für das SMGW transparente Daten
003	SMGW oder aEMT initiiert TLS-Verbindungsabbau	TLS-Verbindungsabbau	aEMT, SMGW	SMGW, aEMT	Informationen zum TLS-Verbindungsabbau

Tabelle 3.7 Beschreibung Kommunikationsszenario „TLSPROXY“

Umzusetzende Anwendungsfälle:

Das SMGW **MUSS** zur Umsetzung der Anwendungsfalles WAF6 über das Kommunikationsszenario "TLSPROXY" mit dem aktiven EMT kommunizieren. [REQ.WAN.Kommunikationsszenarien.100]

3.2.3.7. WAKEUP

Die folgende Abbildung skizziert den Ablauf zur Initiierung einer TLS-Verbindung mit Hilfe des Wake-Up-Services.

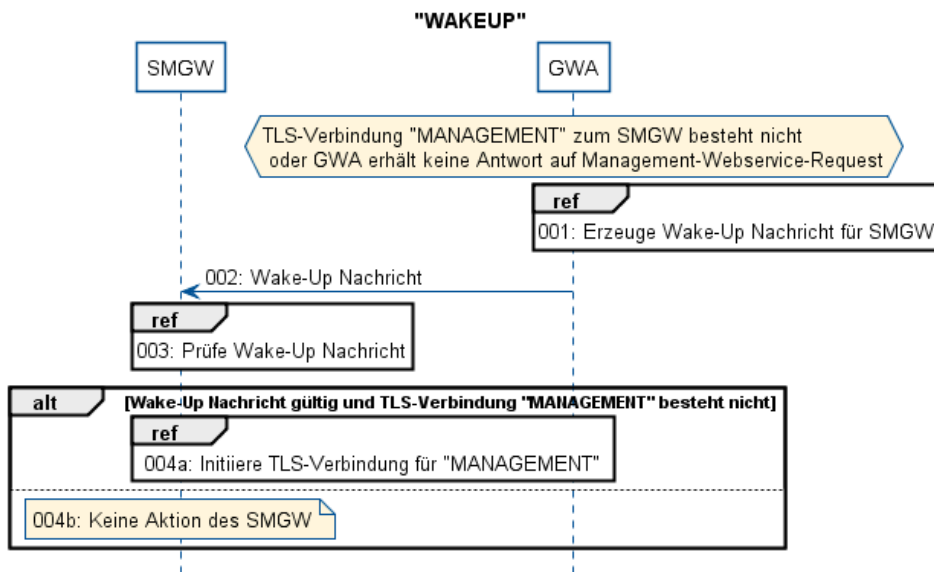


Abbildung 3.7. Sequenzdiagramm für Anwendungsfall und Kommunikationsszenario „WAKEUP“

Vorbedingung:

Es besteht keine TLS-Verbindung vom Typ "MANAGEMENT" zwischen SMGW und GWA. Das SMGW ist für den Wake-Up-Service durch den GWA kommunikativ erreichbar.

Rolle des SMGW:

Wake-Up-Empfänger

Schritt	Ereignis	Aktivität	Sender oder Initiator	Empfänger	Ausgetauschte Daten
001	GWA benötigt eine „MANAGEMENT“ Verbindung zum SMGW	GWA erstellt ein Wake-Up-Paket für das SMGW	-	-	-
002	GWA hat Wake-Up Nachricht erstellt	GWA sendet Wake-Up Nachricht an SMGW	GWA	SMGW	Wake-Up Paket
003	SMGW empfängt Wake-Up Paket	SMGW verarbeitet Wake-Up Nachricht	-	-	-
004a	Gültige Wake-Up Nachricht empfangen	SMGW initiiert TLS-Verbindung Typ "MANAGEMENT"	SMGW	GWA	Informationen zum TLS-Verbindungsaufbau
004b	Ungültige Wake-Up Nachricht empfangen	Keine weitere Aktion des SMGW	-	-	-

Tabelle 3.8 Beschreibung Kommunikationsszenario „WAKEUP“

Umzusetzende Anwendungsfälle:

Das SMGW **MUSS** zur Umsetzung der Anwendungsfalles WAF7 über das Kommunikationsszenario WAKEUP mit dem GWA kommunizieren. [REQ.WAN.Kommunikationsszenarien.110]

3.2.4. Sicherung der Kommunikationsverbindungen in das WAN

3.2.4.1. Anforderungen an TLS bei WAN Verbindungen

Gemäß den Anforderungen aus dem Schutzprofil [PP-0073] **MÜSSEN** die Kommunikationsverbindungen des SMGW oberhalb der Transportschicht mittels TLS abgesichert werden. [REQ.WAN.TlsSicherung.10]

Für die TLS-Kommunikation mit Teilnehmern im WAN **MUSS** das SMGW immer in der Rolle des TLS-Client und die Gegenstelle in der Rolle des TLS-Servers agieren. [REQ.WAN.TlsSicherung.20]

Dabei **MUSS** immer eine beidseitig mittels Zertifikaten authentifizierte TLS-Verbindung aufgebaut werden. [REQ.WAN.TlsSicherung.30]

Das SMGW **MUSS** für die Kommunikation im WAN Endnutzer-Zertifikate aus der Smart Metering Public Key Infrastruktur gemäß [TR-03109-4] und [SM-PKI-CP] verwenden. [REQ.WAN.TlsSicherung.40]

Das SMGW **DARF KEINE** TLS-Verbindungen akzeptieren, die von Teilnehmern aus dem WAN initiiert werden. [REQ.WAN.TlsSicherung.50] Das SMGW kann jedoch über den Wake-Up Dienst (siehe ▶Abschnitt 3.2.6.3) veranlasst werden, eine TLS-Verbindung zum GWA aufzubauen.

Das SMGW **MUSS** gleichzeitig über zwei oder mehr TLS-Verbindungen mit dem GWA kommunizieren können (z.B. zum Management des Gateways und zur Fehlersignalisierung bzw. Alarmierung, siehe ▶Abschnitt 3.2.2). [REQ.WAN.TlsSicherung.60]

Das SMGW **DARF KEINE** ungültigen TLS-Zertifikate verwenden. [REQ.WAN.TlsSicherung.70]

Falls die Systemzeit gemäß ▶REQ.WAF2.Zeitsynchronisation.50 nicht synchronisiert ist, **SOLL** das SMGW die zeitlichen Gültigkeitsprüfung des Zertifikates mit der Systemzeit durch eine Plausibilisierung mit einer anderen Zeitinformaton aus dem SMGW durchführen. [REQ.WAN.TlsSicherung.80]³

³ Beispielsweise Firmware-Datum, Zeitstempel des letzten System-Log-Eintrages.

3.2.4.2. Inhaltsdatensicherung mittels CMS

Zur Sicherung der Inhaltsdaten im WAN **MUSS** das SMGW gemäß [PP-0073] sicherstellen, dass gesendete und empfangene Inhaltsdaten mit CMS für den Endempfänger verschlüsselt und vom Absender signiert sind; ausgenommen sind die Inhaltsdaten zur Zeitsynchronisation und zum Firmware-Download innerhalb einer TLS-Verbindung zum GWA. [REQ.WAN.CmsSicherung.10] Inhaltsdaten einer HTTP-Nachricht sind gemäß [RFC7230] die Daten im "message-body" (auch als "Content" bezeichnet).

Das SMGW **MUSS** die CMS-Datenstrukturen gemäß der Detailspezifikation ☞ CMS verarbeiten und erzeugen können. [REQ.WAN.CmsSicherung.20]

Das SMGW **DARF KEINE** ungültigen Signatur- und Verschlüsselungs-Zertifikate verwenden. [REQ.WAN.CmsSicherung.30]

Falls die Systemzeit gemäß ▶REQ.WAF2.Zeitsynchronisation.50 nicht synchronisiert ist, **SOLL** das SMGW die zeitlichen Gültigkeitsprüfung von Signatur- und Verschlüsselungs-Zertifikaten mit der Systemzeit durch eine Plausibilisierung mit einer anderen Zeitinformation aus dem SMGW durchführen. [REQ.WAN.CmsSicherung.40]³

3.2.4.3. Absicherung des Wake-Up-Dienstes

Es existieren keine Anforderungen an den Transportweg des Wake-Up-Pakets. Das Paket wird über eine im SMGW verbaute WAN-Schnittstelle empfangen. Diese Schnittstelle ist nicht zwangsläufig identisch mit der WAN-Schnittstelle über die anschließend auch die TLS-Verbindung zum GWA aufgebaut wird.

1. Um das SMGW vor Angriffen aus dem WAN auf den Wake-Up-Dienst zu schützen, gelten für die Verarbeitung des Wake-Up-Paketes folgende Anforderungen (in dieser Reihenfolge):
 - a. Das SMGW **MUSS** prüfen, dass die Version, Header-Kennzeichnung und Länge des Paketes mit den Vorgaben in der Detailspezifikation ☞ Datenstruktur der Wake-Up-Nachricht übereinstimmt. [REQ.WAN.WakeUpSicherung.10]
 - b. Das SMGW **MUSS** prüfen, dass die Identifikation des Empfängers im Wake-Up-Paket mit der herstellerübergreifend eindeutigen Identifikation des SMGW (Inhaber der SM-PKI-Zertifikate des SMGW) übereinstimmt. [REQ.WAN.WakeUpSicherung.20]
 - c. Das SMGW **SOLL** Wake-Up-Pakete ignorieren, die innerhalb kurzer Zeit (30s) identisch empfangen wurden. [REQ.WAN.WakeUpSicherung.30]
 - d. Sofern die Systemzeit des SMGW mit dem Zeitserver des GWA synchronisiert ist, **MUSS** das SMGW prüfen, dass der Zeitstempel des Wake-Up-Paketes nicht mehr als +/-30s von der Systemzeit abweicht. [REQ.WAN.WakeUpSicherung.40] Dies soll das Wiederverwenden des Paketes zu einem späteren Zeitpunkt verhindern.
 - e. Das SMGW **MUSS** mit dem öffentlichen Schlüssel aus dem GWA_WAN_SIG_CRT die Signatur des Wake-Up-Paketes prüfen, um festzustellen, ob das Paket vom GWA stammt. [REQ.WAN.WakeUpSicherung.50]
 - f. Das SMGW **SOLL** durch Beschränkung der Anzahl von Signaturprüfungen (innerhalb einer Minute) die Verfügbarkeit des Sicherheitsmodules gewährleisten. [REQ.WAN.WakeUpSicherung.60]
2. Das SMGW **DARF** Wake-Up-Pakete **NICHT** verarbeiten, die die Prüfungen unter ▶1 nicht bestanden haben. [REQ.WAN.WakeUpSicherung.70] Es wird kein Feedback zum Sender zurückgeschickt.



ICS.WAN.WakeUpSicherung.10

Der GWH **MUSS** im ICS deklarieren, auf welche Rate (pro Minute) das SMGW die Nutzung des Sicherheitsmoduls für die Wake-Up-Validierung begrenzt. 0: Falls die Rate nicht begrenzt wird.



ICS.WAN.WakeUpSicherung.20

Der GWH **MUSS** im ICS deklarieren, ob identische Wake-Up-Pakete innerhalb von 30s erkannt und verworfen werden.

3.2.5. Kommunikationsprofile für die WAN-Kommunikation

Ein WAN-Kommunikationsprofil legt die Parameter für die Kommunikation zu einem EMT im WAN oder dem GWA fest.

Das SMGW **MUSS** die folgenden Parameter innerhalb von WAN-Kommunikationsprofilen akzeptieren: [REQ.WAN.Kommunikationsprofil.10]

Parameter	Datentyp / Wertebereich	Beschreibung
Bezeichner	Alphanummerisch	Der im SMGW eindeutige Bezeichner des WAN-Kommunikationsprofils.
Kommunikationsszenario	Eines aus: MANAGEMENT ADMIN-SERVICE INFO-REPORT NTP-TLS NTP-HTTPS	Legt das Kommunikationsszenario fest.
Rolle des Kommunikationspartners	Einer aus: GWA EMT	Legt die Rolle des Kommunikationspartners im WAN fest.
Adresse(n) des EMT oder des GWA	1..n URI	Legt eine oder mehrere Adressen fest, an denen der EMT oder GWA erreichbar ist und zu der eine ein TLS-Sitzung auf TLS-Verbindung vom SMGW aufgebaut werden muss.
Keepalive ⁴	Ja/Nein	Legt fest, ob die TLS-Verbindung dauerhaft aufrechterhalten werden soll, auch wenn die Aktion, die zum Aufbau geführt hat, nicht mehr gegenwärtig ist. Die TLS-Verbindung wird erst dann geschlossen, wenn die maximale Sitzungslänge erreicht ist. Im anderen Fall wird die TLS-Verbindung geschlossen, sobald die Aktion beendet ist.
Wiederholung im Fehlerfall (optional)	0..n	Anzahl der Verbindungsaufbauversuche im Fehlerfall. Führen alle Versuche zu einem Fehler, so muss das Ereignis im System-Log eingetragen werden. (0: Keine Wiederholungen im Fehlerfall)
Wartezeit im Fehlerfall (optional)	1..n Sekunden	Die Wartezeit zwischen Verbindungsaufbauversuchen.
Wartezeit im Leerlauf	0..n Sekunden	Nach Ablauf der Zeit im Leerlauf, wird die TLS-Verbindung wieder abgebaut. Der Wert 0 deaktiviert den Abbau im Leerlauf.
Maximale Sitzungslänge (optional)	30..172800 Sekunden	Die maximale Zeit, die eine TLS-Sitzung aufrechterhalten werden soll. Ein Wert größer als 48h darf vom SMGW nicht akzeptiert werden.
Zertifikat des Kommunikationspartners für die TLS-Authentifizierung	GWA_WAN_TLS_CERT oder EMT_WAN_TLS_CERT	Das Zertifikat des GWA oder EMT für die TLS-Authentifizierung des GWA oder EMT durch das SMGW.

⁴ Sofern die Funktion vom SMGW unterstützt wird (s. ▶ICS.WAN.Kommunikationsprofil.20).

Parameter	Datentyp / Wertebereich	Beschreibung
Zertifikat des Kommunikationspartners für die Signierung der Inhaltsdaten	GWA_WAN_SIG_CRT oder EMT_WAN_SIG_CRT	Das Zertifikat des GWA oder EMT für Signierung von Inhaltsdaten, die vom GWA oder EMT durchgeführt werden muss.
Zertifikat des Kommunikationspartners für den Schlüsseltransport	GWA_WAN_ENC_CRT oder EMT_WAN_ENC_CRT	Das Zertifikat des GWA oder EMT für den Schlüsseltransport von symmetrischen Schlüsseln für die Verschlüsselung von Inhaltsdaten, die vom SMGW durchgeführt werden muss.
SubCA-Zertifikat zu den Zertifikaten des Kommunikationspartners	SUB-CA_WAN_SIG_CRT	Das Zertifikat der SubCA, welche die Zertifikate des GWA oder EMT innerhalb dieses Profils ausgestellt hat.
Zertifikat des SMGW für die TLS-Authentifizierung ⁵	GW_WAN_TLS_CRT	Ein Zertifikat des SMGW für die TLS-Authentifizierung durch den GWA oder EMT.
Zertifikat des SMGW für die Signierung von Inhaltsdaten ⁵	GW_WAN_SIG_CRT	Ein Zertifikat des SMGW das für die Signierung von Inhaltsdaten durch das SMGW verwendet werden muss.
Zertifikat des SMGW für den Schlüsseltransport ⁵	GW_WAN_ENC_CRT	Ein Zertifikat des SMGW, das für den Schlüsseltransport von symmetrischen Schlüsseln für die Entschlüsselung von Inhaltsdaten im SMGW verwendet werden muss.

Tabelle 3.9 Durch WAN-Kommunikationsprofile festzulegende Parameter

Werden optionale Parameter nicht vom GWA übermittelt, so werden die Werte vom SMGW bestimmt.

Das SMGW **KANN** weitere Parameter für WAN-Kommunikationsprofile unterstützen. [REQ.WAN.Kommunikationsprofil.20]

Das SMGW **DARF** dem GWA die Möglichkeit bereitstellen, die Zertifikate des SMGW mithilfe einer vom WAN-Kommunikationsprofil unabhängigen Datenstruktur einzuspielen. [REQ.WAN.Kommunikationsprofil.30] In diesem Fall entfällt die Notwendigkeit diese Parameter als Teil des WAN-Kommunikationsprofils zu akzeptieren.

Vor der Aktivierung der Kommunikationsprofile muss das SMGW die folgenden Punkte sicherstellen:

- Das SMGW **MUSS** sicherstellen, dass der Rolle EMT in den WAN-Kommunikationsprofilen ausschließlich das Kommunikationsszenario INFO-REPORT zugeordnet wird. [REQ.WAN.Kommunikationsprofil.40]⁶
- Das SMGW **MUSS** sicherstellen, dass der Rolle GWA in den WAN-Kommunikationsprofilen ausschließlich die Kommunikationsszenarien MANAGEMENT, ADMIN-SERVICE, NTP-HTTPS, NTP-TLS zugeordnet werden. [REQ.WAN.Kommunikationsprofil.50]

Das SMGW **MUSS** sicherstellen, dass jederzeit mindestens ein WAN-Kommunikationsprofil mit der Rolle GWA und dem Kommunikationsszenario MANAGEMENT aktiviert ist. [REQ.WAN.Kommunikationsprofil.60] Das SMGW **SOLL** sicherstellen, dass jederzeit mindestens ein WAN-Kommunikationsprofil mit der Rolle GWA und dem Kommunikationsszenario ADMIN-SERVICE und ein Kommunikationsprofil für die Zeitsynchronisation aktiviert ist. [REQ.WAN.Kommunikationsprofil.62]

Das SMGW **MUSS** die Deaktivierung oder Löschung des WAN-Kommunikationsprofils verhindern, solange noch ein aktives Auswertungsprofil auf das zu deaktivierende WAN-Kommunikationsprofil verweist. [REQ.WAN.Kommunikationsprofil.70]

Wird eine der Anforderungen aus ▶REQ.WAN.Kommunikationsprofil.50 oder ▶REQ.WAN.Kommunikationsprofil.60 nicht erfüllt, so **DARF** das SMGW das WAN-Kommunikationsprofil **NICHT** aktivieren. [RE-

⁵ Sofern gemäß ▶ICS.WAN.Kommunikationsprofil.30 keine gesonderte Datenstruktur verwendet wird.

⁶ Das Kommunikationsszenario TLSPROXY mit der Rolle des aktiven EMT wird in ▶Abschnitt 3.4.5.3 beschrieben.

Q.WAN.Kommunikationsprofil.80] In diesem Fall **MUSS** das SMGW einen entsprechenden Eintrag im System-Log protokollieren und den GWA darüber informieren. [REQ.WAN.Kommunikationsprofil.90]

Zu der möglichen Modellierung der Datenstruktur der WAN-Kommunikationsprofile siehe ▶Abschnitt 3.2.6.1.



ICS.WAN.Kommunikationsprofil.10

Der GWH **MUSS** im ICS alle weiteren Parameter für WAN-Kommunikationsprofile beschreiben, die gemäß ▶REQ.WAN.Kommunikationsprofil.20 vom SMGW zusätzlich unterstützt werden.



ICS.WAN.Kommunikationsprofil.20

Der GWH **MUSS** im ICS beschreiben, ob das SMGW den Parameter "Keepalive" aus ▶Tabelle 3.9 unterstützt.



ICS.WAN.Kommunikationsprofil.30

Der GWH **MUSS** im ICS beschreiben, ob das SMGW die Datenstruktur gemäß ▶REQ.WAN.Kommunikationsprofil.30 akzeptiert und wie diese Datenstruktur aufgebaut ist.



ICS.WAN.Kommunikationsprofil.40

Der GWH **MUSS** im ICS beschreiben, ob das SMGW sicherstellt, dass jederzeit mindestens ein WAN-Kommunikationsprofil vom Typ ADMIN-SERVICE und eines für die Zeitsynchronisation aktiviert ist.

3.2.6. WAN-Kommunikationsprotokolle

Die in ▶Abschnitt 3.2.3 definierten Kommunikationsszenarien sind aus einer Kombination von Kommunikationsprotokollen zusammengesetzt ("Protokollstapel"), die sich untergliedern in:

1. Semantische Vorgaben zur Datenmodellierung (Profile)
2. Transfersyntax für Datenstrukturen
3. Inhaltsdatensicherung
4. Zugriffsprotokoll zur Abfrage und Darstellung der Daten
5. Transportsicherung
6. Transportprotokoll

Die Kommunikation des SMGW über das WAN mit dem GWA bzw. mit EMT wird über die in ▶Abbildung 3.8 dargestellten Protokollstapel durchgeführt:

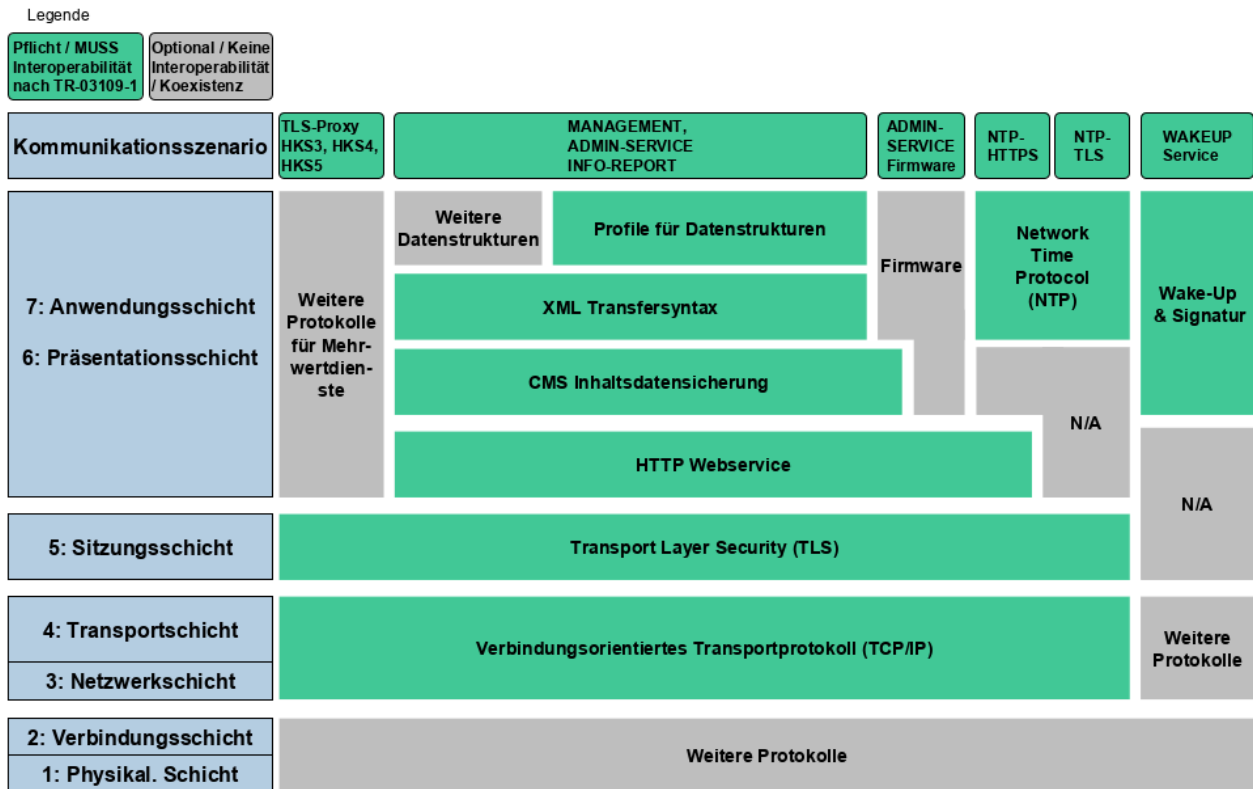


Abbildung 3.8. Protokollstapel für die WAN-Kommunikation



Anmerkung

Anmerkung: Die Protokolle unterhalb der Netzwerkschicht werden von dieser Technischen Richtlinie nicht vorgegeben.

3.2.6.1. Datenmodellierung

Die Identifikation der *Messgrößen* und Messarten für die Messwertübermittlung an den EMT **MUSS** mit *OBIS-Kennzahlen* aus den Standards [EN62056-6-1] und [EN13757-1] geschehen. [REQ.WAN.Datenmodell.10]

Die Modellierung der Datenstrukturen des SMGW für den Versand von Messwerten an den EMT **KANN** mit Hilfe von COSEM Interface-Klassen aus [VDE0418-63-8] geschehen. [REQ.WAN.Datenmodell.20] (siehe ▶ICS.WAN.Datenmodell.10)

Die Modellierung der Datenstrukturen des SMGW für die Administration **KANN** mit Hilfe von COSEM Interface-Klassen und OBIS-Kennzahlen aus [VDE0418-63-8] geschehen. [REQ.WAN.Datenmodell.30] (siehe ▶ICS.WAN.Datenmodell.20)

Das SMGW **MUSS** die Datenstrukturen, die sich aus den Anwendungsfällen aus ▶Abschnitt 3.2.2 ableiten, in der Transfersyntax XML nach [XML1.0] mit UTF-8 Codierung verarbeiten und versenden können. [REQ.WAN.Datenmodell.40]



ICS.WAN.Datenmodell.10

Der GWH **MUSS** im ICS deklarieren, ob die Modellierung der Datenstrukturen des SMGW für den Messwertversand mit Hilfe von COSEM Interface-Klassen aus dem Standard [VDE0418-63-8] geschieht.

**ICS.WAN.Datenmodell.20**

Der GWH **MUSS** im ICS deklarieren, ob die Modellierung der Datenstrukturen des SMGW für die Administration mit Hilfe von COSEM Interface-Klassen aus dem Standard [VDE0418-63-8] geschieht.

**ICS.WAN.Datenmodell.30**

Der GWH **MUSS** im ICS deklarieren, mit welchen XML-Schemata die gesendeten und empfangenen XML-Inhaltsdaten zur Umsetzung von WAF1 über WKS MANAGEMENT validiert werden können. Sofern diese XML-Schemata nicht öffentlich zugänglich sind, **MUSS** der GWH sie inkl. Dokumentation zur Anwendung als Anlage zum ICS bereitstellen.


**ICS.WAN.Datenmodell.40**

Der GWH **MUSS** im ICS deklarieren, mit welchen XML-Schemata die gesendeten XML-Inhaltsdaten zur Umsetzung von WAF5 über WKS INFO-REPORT vom SMGW validiert werden können. Sofern diese XML-Schemata nicht öffentlich zugänglich sind, **MUSS** der GWH sie als Anlage inkl. Dokumentation zur Anwendung zum ICS bereitstellen.

**ICS.WAN.Datenmodell.50**

Der GWH **MUSS** im ICS deklarieren, mit welchen XML-Schemata die gesendeten und empfangenen XML-Inhaltsdaten zur Umsetzung von WAF2, WAF3 über WKS ADMIN-SERVICE validiert werden können. Sofern diese XML-Schemata nicht öffentlich zugänglich sind, **MUSS** der GWH sie als Anlage inkl. Dokumentation zur Anwendung zum ICS bereitstellen.

3.2.6.2. Webservices

Das SMGW **MUSS** den Zugriff auf Ressourcen des SMGW über das Kommunikationsszenario WKS MANAGEMENT mit einem RESTful Webservice Protokoll gemäß Detailspezifikation  RESTful Webservice unterstützen. [REQ.WAN.Webservice.10]

Das SMGW **MUSS** die Zugriffsberechtigungen gemäß ▶Abschnitt 4.5.3 und [PP-0073] prüfen und bei fehlender Berechtigung den Zugriff auf die Ressource unmittelbar mit einer Fehlermeldung beenden. [REQ.WAN.Webservice.20]

Die Statuscodes und eventuell im Response Body vorhandene Detailinformation zum aufgetretenen Fehler **MUSS** das SMGW im System-Log aufzeichnen. [REQ.WAN.Webservice.30]

Das SMGW **MUSS** Nachrichten über WKS ADMIN-SERVICE an den GWA mittels HTTP "POST" Request bereitstellen. [REQ.WAN.Webservice.40]

Das SMGW **MUSS** Nachrichten über WKS INFO-REPORT an den EMT mittels HTTP "POST"-Request bereitstellen. [REQ.WAN.Webservice.50]

Das SMGW **MUSS** im Webservice-Request bzw. in der Webservice-Response mitteilen, welche Struktur die Inhaltsdaten besitzen und welchem XML-Schema die (unverschlüsselten) Datenstrukturen der Anwendungsdaten entsprechen. [REQ.WAN.Webservice.60]

Das SMGW **SOLL** innerhalb von 30s im WKS MANAGEMENT eine Anfrage beantworten. [REQ.WAN.Webservice.70]

**ICS.WAN.Webservice.10**

Der GWH **MUSS** im ICS deklarieren, über welche URIs und HTTP-Methoden der GWA auf die Ressourcen zur Umsetzung von WAF1 über WKS MANAGEMENT zugreifen kann.

**ICS.WAN.Webservice.20**

Der GWH **MUSS** im ICS deklarieren, mit welchem "Content-Type" das SMGW im WKS MANAGEMENT, WKS ADMIN-SERVICE, WKS NTP-HTTPS Inhaltsdaten verarbeitet und versendet und welches XML-Schema diesen Content-Types zugeordnet ist.

**ICS.WAN.Webservice.30**


Der GWH **MUSS** im ICS deklarieren, mit welchem "Content-Type" das SMGW im WKS INFO-REPORT Inhaltsdaten versendet und welches XML-Schema diesen Content-Types zugeordnet ist.

**ICS.WAN.Webservice.40**

Der GWH **MUSS** im ICS deklarieren, ob die synchrone Beantwortung von Anfragen an das SMGW im WKS MANAGEMENT länger als 30s dauern kann und in einer Anlage zum ICS beschreiben, wie der GWA dies erkennen kann.

3.2.6.3. Wake-Up-Dienst und Protokoll

Der GWA kann dem SMGW über das Wake-Up-Protokoll eine Anforderung übermitteln, eine MANAGEMENT-Verbindung zum GWA herzustellen.

Das SMGW **MUSS** die Prüfung der Wake-Up-Nachricht mit der Datenstruktur der Detailspezifikation  Datenstruktur der Wake-Up-Nachricht nach den Anforderungen in ▶Abschnitt 3.2.4.3 durchführen. [REQ.WKS.WakeUp.10]

Das SMGW **SOLL** nach erfolgreicher Prüfung der Wake-Up-Nachricht innerhalb der in ▶ICS.WKS.WakeUp.10 angegebenen Zeitdauer eine MANAGEMENT-Verbindung zum GWA initiieren. [REQ.WKS.WakeUp.20]

**ICS.WKS.WakeUp.10**

Der GWH **MUSS** im ICS deklarieren, innerhalb welcher Zeit (in Sekunden) das SMGW nach Empfang einer gültigen Wake-Up-Nachricht eine MANAGEMENT-Verbindung zum GWA initiiert.

3.2.6.4. Zeitsynchronisation-Protokoll

Das SMGW **MUSS** die Zeitsynchronisation mit den Datenstrukturen und Anforderungen an die Verarbeitung des NTP-Protokolles nach [RFC5905] durchführen. [REQ.WAN.Zeitsynchronisation.10]

Das SMGW **DARF NICHT** andere Technologien (wie bspw. DCF77) zur Zeitsynchronisation verwenden. [REQ.WAN.Zeitsynchronisation.20]

Das SMGW **MUSS** die für das NTP-Protokoll notwendige Bestimmung der Sende- und Empfangszeitpunkte der NTP-Nachrichten erst durchführen, nachdem die TLS-gesicherte Verbindung aufgebaut ist, damit die Zeit, die für den Verbindungsaufbau benötigt wird nicht die RTT-Messung beeinflusst. [REQ.WAN.Zeitsynchronisation.40]

**ICS.WAN.Zeitsynchronisation.10**

Der GWH **MUSS** im ICS beschreiben, ob und mit welchem Mechanismus die Vermeidung der Überlastung des GWA-Zeitserver nach einer Betriebsunterbrechung des SMGW gewährleistet wird.

3.2.6.4.1. Umsetzung von NTP über HTTPS

Die Zeitsynchronisierung erfolgt in diesem Kommunikationsszenario mit einem über einen HTTP-Server erreichbaren Zeitserver.

Das SMGW **MUSS** die NTP-Datenstrukturen als HTTP-Content ohne Inhaltsdatensicherung (CMS) senden und empfangen können. [REQ.WAN.Zeitsynchronisation.50]



Anmerkung

Die Gesamtgröße der übertragenen Pakete (HTTP Header und HTTP Body mit NTP-Nutzinformationen) sollen auf dem Hin- und Rückweg in etwa dieselbe Größe aufweisen, um die Zeitabweichung auf dem Hin- und Rückweg aufgrund unterschiedlicher Paketgrößen möglichst minimal zu halten.

Das SMGW **DARF KEINE** anderen Informationen, als die notwendigen HTTP-Header-Informationen und die NTP-Nachricht nach [RFC5905] über diese Verbindung übertragen. [REQ.WAN.Zeitsynchronisation.60]



ICS.WAN.Zeitsynchronisation.20

Der GWH **MUSS** im ICS deklarieren, ob das SMGW NTP über HTTPS unterstützt.

3.2.6.4.2. Umsetzung von NTP über TLS

Das SMGW **DARF KEINE** anderen Informationen, als die NTP-Nachricht nach [RFC5905] über diese Verbindung übertragen. [REQ.WAN.Zeitsynchronisation.70]



ICS.WAN.Zeitsynchronisation.30

Der GWH **MUSS** im ICS deklarieren, ob das SMGW NTP-TLS unterstützt.

3.2.6.4.3. Vermeidung von Fehl-Synchronisierungen

Die Round-Trip-Time (RTT) bzw. die gesamte Verzögerung zwischen SMGW und GWA-Zeitserver ist in der Regel für die Genauigkeit der Synchronisation unerheblich, solange gewährleistet ist, dass die Verzögerungen auf dem Hin- und Rückweg vom Zeitserver ungefähr gleich sind. Zur Vermeidung von Fehl-Synchronisationen muss das SMGW jedoch bei jeder Zeitsynchronisation die obere Grenze RTT_{max} beachten.

Das SMGW bestimmt die Zeitabweichung (ZA) zwischen Systemzeit des SMGW und Zeitserver aus den vom NTP-Protokoll bereitgestellten Informationen. Die Festlegung der maximal erlaubten Zeitabweichung (ZA_{max}) der Systemzeit des SMGW von der Zeit des GWA-Zeitserver wird durch die kleinste vom SMGW unterstützte *Registrierperiode* beeinflusst (Siehe ▶ Abschnitt 3.2.7). ZA_{max} kann jedoch nicht beliebig klein gewählt werden, da eine untere Schranke für die maximal erlaubte Round-Trip-Time (RTT_{max}) maßgeblich durch die WAN-Übertragungstechnik bestimmt wird.

Um Delay-Angriffe und Zeitmessungen mit zu langer RTT zu verwerfen, **SOLL** das SMGW die RTT zwischen SMGW und GWA-Zeitserver messen und empfangene NTP-Nachrichten mit $RTT > RTT_{max}$ (mit $RTT_{max} < ZA_{max}$) verwerfen und diese Überschreitung im System-Log protokollieren. [REQ.WAN.Zeitsynchronisation.80]

Um die Systemzeit "synchron" innerhalb der Toleranz ZA_{max} zu halten, **SOLL** das SMGW im Wirkbetrieb die Bedingung $|ZA| + 0,5 * RTT < ZA_{max}$ einhalten. [REQ.WAN.Zeitsynchronisation.90]⁷

Falls eine korrekte Zeitsynchronisierung über einen längeren Zeitraum nicht möglich ist, **MUSS** das SMGW einen Eintrag im Eichlog protokollieren und versuchen den GWA zu benachrichtigen. [REQ.WAN.Zeitsynchronisation.100] Diese Warnung soll verhindern, dass die Systemzeit nicht mehr synchronisiert ist und das SMGW die Anwendungsfälle nicht mehr uneingeschränkt umsetzen kann.

⁷ Im Störfall oder nach einer vorübergehenden Betriebsunterbrechung kann die Prüfung dieser Bedingung entfallen.

**ICS.WAN.Zeitsynchronisation.40**

Der GWH **MUSS** im ICS deklarieren, ob das SMGW die NTP-Nachrichten mit $RTT > RTT_{max}$ nicht für die Zeitsynchronisation verwendet.

**ICS.WAN.Zeitsynchronisation.50**

Der GWH **MUSS** im ICS deklarieren, ob das SMGW die Einhaltung von $|ZA| + 0,5 * RTT < ZA_{max}$ im Wirkbetrieb gewährleistet.

3.2.6.5. Transport von TLS

Um einen zuverlässigen und interoperablen Transport von TLS-Records im WAN zu gewährleisten, **MUSS** das SMGW das TCP/IP Protokoll verwenden. [REQ.WAN.Transport.10]

Das SMGW **MUSS** das TCP/IPv4-Protokoll an der WAN-Schnittstelle für die TLS-Verbindungen zum GWA und EMT verwenden können. [REQ.WAN.Transport.20]

Das SMGW **SOLL** das TCP/IPv6-Protokoll an der WAN-Schnittstelle für die TLS-Verbindungen zum GWA und EMT verwenden können. [REQ.WAN.Transport.30]

Das SMGW **MUSS** dem GWA in der Transport- und/oder TLS-Verbindung signalisieren, welcher Kommunikationspartner und welches Kommunikationsszenario für die TLS-Verbindung erwartet wird. [REQ.WAN.Transport.40]⁸

**ICS.WAN.Transport.10**

Der GWH **MUSS** im ICS deklarieren, ob das SMGW an der WAN-Schnittstelle TLS-Records über TCP/IPv6 transportieren kann.

3.2.7. Zeitführung des SMGW**3.2.7.1. Einleitung**

Das SMGW besitzt eine Systemuhr, die die Systemzeit für die Kommunikationsprotokolle, die Zertifikatsprüfung und Anwendungsfälle des SMGW bereitstellt. Das SMGW synchronisiert die Systemzeit in regelmäßigen Abständen mit einem Zeitserver des GWA. GWA-Zeitserver synchronisieren sich mit den Zeitservern der PTB, die die gesetzliche Zeit bereitstellen.

⁸ Beispielsweise über die vom GWA konfigurierte Transport-Adresse oder einen vereinbarten TLS-Service-Name-Indicator.

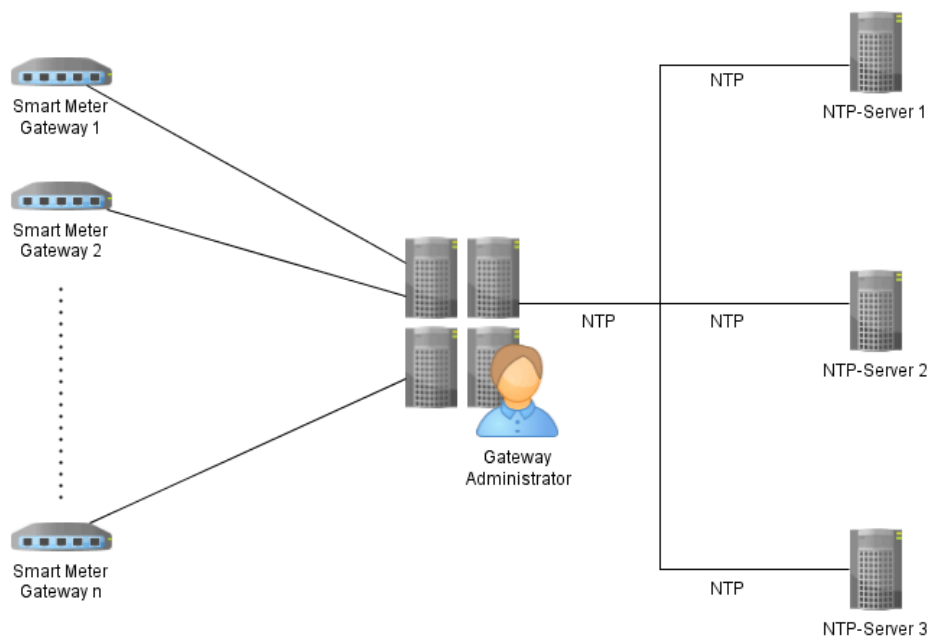


Abbildung 3.9. Zeitsynchronisation zwischen SMGW und GWA-Zeitserver

3.2.7.2. Fehlerbetrachtung der Zeitsynchronisation

Für eine Fehlerbetrachtung im Rahmen dieser Einsatzumgebung müsste das Fehlerkontingent der Strecke SMGW <--> GWA-Zeitserver als auch das der Strecke GWA-Zeitserver <--> PTB-Zeitserver betrachtet werden. Da die Zeitabweichung zwischen GWA-Zeitserver und PTB-Zeitserver auf 0,01 % der kleinsten Registrierperiode oder 90 ms begrenzt ist⁹, wird davon ausgegangen, dass der gesamte Fehler durch die Strecke SMGW <--> GWA-Zeitserver dominiert wird. Damit wird im Folgenden für die Betrachtung des möglichen Fehlers nur die Strecke zwischen SMGW und GWA-Zeitserver betrachtet.

Das SMGW **MUSS** sicherstellen, dass die Zeitabweichung der Systemzeit von der Zeit des Zeitserver des GWA und die Laufzeit der NTP-Nachrichten ("Round Trip Time", RTT) jeweils festgelegte Schwellwerte nicht überschreiten. [REQ.WAF2.Zeitsynchronisation.10]¹⁰

Das SMGW **KANN** eine Gangreserve für die Systemuhr besitzen. [REQ.WAF2.Zeitsynchronisation.20]

Die Gangreserve der Systemuhr kann über einen Hardware-Baustein (Real-Time-Clock, RTC) realisiert werden, z.B. mit Kondensator/Batteriepufferung im Falle des Ausfalles der Energieversorgung des SMGW.

Falls die Systemuhr des SMGW eine Gangreserve besitzt, **MUSS** das SMGW in der Lage sein, bei Wiederaufnahme des normalen Betriebs zu erkennen, ob die Dauer des Ausfalles der Versorgungsspannung der Systemuhr größer war als die garantierte Gangreserve. [REQ.WAF2.Zeitsynchronisation.30] In diesem Fall kann es zu einer unzulässigen Abweichung der Systemzeit von der gesetzlichen Zeit gekommen sein und ein Eintrag in das Eichlog hat zu erfolgen. Dabei soll die garantierte Gangreserve höchstens so lang gewählt werden, dass unter Berücksichtigung der Langzeitstabilität des Uhrenbausteins die hochgerechnete Abweichung bei Ablauf der Gangreserve gerade die Fehlergrenze (siehe ▶REQ.WAF2.Zeitsynchronisation.50) erreicht hat.

Das SMGW **MUSS** eine Zeitsynchronisation mit dem Zeitserver des GWA durchführen, sofern die Gangreserve der Systemzeit nach einer Betriebsunterbrechung des SMGW nicht gewährleistet werden kann. [REQ.WAF2.Zeitsynchronisation.40]

Das SMGW **MUSS** die Systemzeit regelmäßig mit einem Zeitserver des GWA, der die gesetzliche Zeit bereitstellt synchronisieren, dass die Abweichung zur Zeit des GWA-Zeitserver stets weniger als oder gleich 27 Se-

⁹ Zu Anforderungen an den Zeitserver siehe [TR-03109-6].

¹⁰ z.B. durch ausreichend häufige Zeitsynchronisation

kunden beträgt. Die Systemzeit wird dann als *synchronisiert* bezeichnet. Diese Fehlergrenze entspricht 3 % von 15 Minuten Registrierperiodendauer. [REQ.WAF2.Zeitsynchronisation.50]

Das SMGW **SOLL** die Systemzeit regelmäßig so synchronisieren, dass die Abweichung zur Zeit des GWA-Zeit-servers, stets weniger als oder gleich 9 Sekunden beträgt. [REQ.WAF2.Zeitsynchronisation.60]

Im Falle der Überschreitung der Fehlergrenze nach ▶REQ.WAF2.Zeitsynchronisation.50 (Zustand "nicht-synchronisiert") **MUSS** das SMGW das Ereignis im System-Log und im Eichlog protokollieren und den GWA darüber informieren. [REQ.WAF2.Zeitsynchronisation.70]

Das SMGW **KANN** auf eine Prüfung der Bedingung in ▶REQ.WAN.Zeitsynchronisation.90 verzichten, solange die Systemzeit nicht mit der gesetzlichen Zeit synchronisiert ist. [REQ.WAF2.Zeitsynchronisation.80]

Sofern ein SMGW eine gültige Uhrzeit nicht (mehr) sicherstellen kann **MUSS** das SMGW eine Zeitsynchronisierung durchführen. [REQ.WAF2.Zeitsynchronisation.90] Beispielsweise nach einem Neustart ohne oder bei erschöpfter Gangreserve.



ICS.WAF2.Zeitsynchronisation.10

Der GWH **MUSS** im ICS deklarieren, ob die Systemuhr eine Gangreserve besitzt und in der Anlage zum ICS beschreiben, welche garantierte Dauer diese Gangreserve in Stunden hat (0, keine Gangreserve).



ICS.WAF2.Zeitsynchronisation.20

Der GWH **MUSS** im ICS deklarieren, ob das SMGW die Abweichung der Systemzeit zur Zeit des GWA-Zeit-servers $\leq 9s$ gewährleistet.

3.2.8. Netzwerkdienstservice

Der Netzwerkdienstservice erlaubt die Bereitstellung von Status- und Diagnoseinformationen über die WAN-Verbindung des SMGW für den GWA oder einen EMT. Anforderungen an die interoperable Umsetzung dieses Dienstes finden sich in der Detailspezifikation [Netzwerkdienstservice](#). Grundsätzlich sind auf Basis der durch den GWH gewählten Sicherheitsarchitektur auch andere Umsetzungen zur Bereitstellung von Netzwerkdienstdaten (bspw. PP-konform als Dienst des im Gehäuse des SMGW befindlichen separierten WAN-Kommunikationsadapters) möglich.

Die Implementierung des Netzwerkdienstservice ist für den GWH optional. Sollte das SMGW den Netzwerkdienstservice gemäß ▶ICS.NDS.Umsetzung.10 implementieren, sind die Anforderungen der Detailspezifikation Netzwerkdienstservice als normativ zu betrachten, ansonsten sind sie informativ.



ICS.NDS.Umsetzung.10

Der GWH **MUSS** im ICS angeben, ob das SMGW einen Netzwerkdienstservice gemäß der Detailspezifikation [Netzwerkdienstservice](#) implementiert.

3.2.9. Selbsttests

- Das SMGW **MUSS** auf Anforderung und regelmäßig selbstständig die Integrität und Authentizität der Firmware/Software vor absichtlicher Veränderung prüfen. [REQ.WAN.Selbsttest.10]
- Das SMGW **SOLL** auf Anforderung und regelmäßig selbstständig die Integrität der Firmware, Konfigurations-Parameter, gespeicherten Messwerte und weiterer Daten vor zufälligen und unbeabsichtigten Veränderungen prüfen. [REQ.WAN.Selbsttest.20]
- Das SMGW **SOLL** auf Anforderung und regelmäßig selbstständig die Plausibilität der Systemzeit und der Einhaltung der Zeitabweichung durch Zeitsynchronisation prüfen. [REQ.WAN.Selbsttest.30]

- Das SMGW **SOLL** auf Anforderung und regelmäßig selbstständig die Zuverlässigkeit der LMN-Kommunikation prüfen. [REQ.WAN.Selbsttest.40]
- Das SMGW **SOLL** auf Anforderung und regelmäßig selbstständig die physische Manipulation des SMGW prüfen. [REQ.WAN.Selbsttest.50]
- Das SMGW **SOLL** auf Anforderung und regelmäßig selbstständig die kommunikative Erreichbarkeit der EMTs durch das SMGW prüfen. [REQ.WAN.Selbsttest.60]

**ICS.WAN.Selbsttest.10**

Der GWH **MUSS** im ICS angeben, ob das SMGW eine Selbsttest-Funktion gemäß ▶REQ.WAN.Selbsttest.20 bereitstellt.

**ICS.WAN.Selbsttest.20**

Der GWH **MUSS** im ICS angeben, ob das SMGW eine Selbsttest-Funktion für die Plausibilität und Einhaltung der Zeitabweichung der Systemzeit gemäß ▶REQ.WAN.Selbsttest.30 bereitstellt.

**ICS.WAN.Selbsttest.30**

Der GWH **MUSS** im ICS angeben, ob das SMGW eine Selbsttest-Funktion für die Zuverlässigkeit der LMN-Kommunikation gemäß ▶REQ.WAN.Selbsttest.40 bereitstellt.

**ICS.WAN.Selbsttest.40**

Der GWH **MUSS** im ICS angeben, ob das SMGW eine Selbsttest-Funktion für die physische Manipulation des SMGW gemäß ▶REQ.WAN.Selbsttest.50 bereitstellt.

**ICS.WAN.Selbsttest.50**

Der GWH **MUSS** im ICS angeben, ob das SMGW eine Selbsttest-Funktion für die kommunikative Erreichbarkeit der EMTs gemäß ▶REQ.WAN.Selbsttest.60 bereitstellt.

3.3. Vorgaben an die Kommunikationsverbindungen in das LMN

3.3.1. Übersicht

Das SMGW kommuniziert im LMN mit einem oder mehreren drahtgebunden oder drahtlos angeschlossenen Zählern, um von diesen Messwerte zu erhalten.

Anwendungsfälle, die eine LMN-Kommunikation erfordern, werden in ▶Abschnitt 3.3.2 skizziert. Die zur Realisierung dieser Anwendungsfälle notwendigen Kommunikationsszenarien werden in ▶Abschnitt 3.3.3 definiert.

Die Anforderungen an die Sicherung der Kommunikation im LMN werden in ▶Abschnitt 3.3.4 beschrieben.

Die Festlegungen zu den Kommunikationsprotokollen, die für drahtgebundene und drahtlose Zähler vom SMGW mindestens unterstützt werden müssen, folgen in ▶Abschnitt 3.3.5.

3.3.2. Anwendungsfälle an der LMN-Schnittstelle

Dieser Abschnitt listet diejenigen Anwendungsfälle auf (gekennzeichnet mit dem Kürzel LAF), die zwingend eine Kommunikation des SMGW mit Zählern im LMN erfordern. Das SMGW **KANN** weitere Anwendungsfälle an der LMN-Schnittstelle unterstützen. [REQ.LMN.Anwendungsfalle.10]

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

1. LMN-Zählerverwaltung.
2. Abruf/Empfang von Messwerten.

3.3.2.1. LAF1: LMN Zählerverwaltung

Das SMGW unterstützt die Verwaltung der Zähler im LMN mit folgenden Anwendungsfällen:

- kommunikative Anbindung und Registrierung von Zählern

Das SMGW **MUSS** die kommunikative Anbindung und Registrierung berechtigter Zähler im LMN auf Veranlassung des GWA unterstützen, um Anwendungsfälle an der LMN Schnittstelle zu ermöglichen. [REQ.LMN.Zaehlerverwaltung.10]

- Schlüssel-/Zertifikatsmanagement

Das SMGW erstellt, verteilt, aktiviert und deaktiviert Schlüsselpaare, Zertifikate und symmetrische Schlüssel für die Kommunikation mit Zählern im LMN.

Folgende Aufgaben sind für die bidirektionale Kommunikation mit Zählern notwendig:

- Das SMGW **MUSS** für die initiale kommunikative Anbindung eines bidirektional kommunizierenden Zählers ein Schlüsselpaar nach [TR-03109-3] für die Messeinrichtung erzeugen, damit ein selbstsigniertes Zertifikat für den Zähler erstellen und beides vertraulich und authentisch an den Zähler übermitteln können. [REQ.LMN.Zaehlerverwaltung.20]
- Das SMGW **SOLL** das Schlüsselpaar und das LMN-TLS-Zertifikat des bidirektional kommunizierenden Zählers im Zähler aktualisieren können. [REQ.LMN.Zaehlerverwaltung.30] Die Aktualisierung wird vor Ende der Laufzeit gemäß [TR-03109-3] durch den GWA oder das SMGW initiiert.
- Das SMGW **SOLL** das LMN-TLS-Zertifikat des SMGW in bidirektional kommunizierenden Zählern aktualisieren können. [REQ.LMN.Zaehlerverwaltung.40] Die Aktualisierung wird vor Ende der Laufzeit gemäß [TR-03109-3] durch den GWA oder das SMGW initiiert.
- Das SMGW **SOLL** den zählerindividuellen, gemeinsamen „Master“-Schlüssel für symmetrisch verschlüsselt, bidirektional kommunizierende Zähler über eine TLS-Verbindung gemäß [TR-03109-3] aktualisieren können. [REQ.LMN.Zaehlerverwaltung.50]

3.3.2.2. LAF2: Abruf/Empfang von Messwerten

Das SMGW **MUSS** die in den Zählern gebildeten Messwerte abfragen bzw. periodisch zugeliferte Werte empfangen können. [REQ.LMN.Messwertempfang.10]

Voraussetzung für den Empfang und die Verarbeitung der Messwerte im SMGW ist die vorherige Registrierung und Konfiguration des Zählers im SMGW.

Folgende Varianten der Messwerterfassung lassen sich unterscheiden:

- Einzelabruf von Messwerten

Der Zähler verhält sich passiv und stellt erst dann einen Messwert zur Verfügung, wenn er dazu vom SMGW aufgefordert wird. Das SMGW **MUSS** Einzelabrufe von Messwerten durchführen können. [REQ.LMN.Messwertempfang.20]

Dieser Anwendungsfall erfordert aufgrund des Request-/Response-Kommunikationsmusters eine bidirektionale Verbindung.

- Zulieferung von Messwerten

Das SMGW **MUSS** eine periodische Zulieferung von Messwerten, die vom unidirektional kommunizierenden Zähler unaufgefordert gesendet werden, unterstützen. [REQ.LMN.Messwertempfang.30]

Dieser Anwendungsfall erfordert mindestens eine unidirektionale Verbindung mit einem Zähler als Sender und dem SMGW als Empfänger.

Das SMGW **MUSS** bei der Registrierung bzw. Erfassung abrechnungsrelevanter Messwerte die zeitlichen Anforderungen der technischen Vorgaben nach [MessEG]/[MessEV] einhalten. [REQ.LMN.Messwertempfang.40]



ICS.LMN.Anwendungsfaelle.10

Der GWH **MUSS** im ICS deklarieren, ob über die in LAF1 und LAF2 genannten Anwendungsfälle weitere LMN Anwendungsfälle unterstützt werden. Sofern dies der Fall ist, beschreibt er diese in einer Anlage zum ICS.



ICS.LMN.Anwendungsfaelle.20

Der GWH **MUSS** im ICS deklarieren, ob das SMGW das Schlüsselpaar und das LMN-TLS-Zertifikat des bidirektional kommunizierenden Zählers im Zähler aktualisieren kann.



ICS.LMN.Anwendungsfaelle.30

Der GWH **MUSS** im ICS deklarieren, ob das SMGW das Schlüsselpaar und das LMN-TLS-Zertifikat des SMGW im Zähler aktualisieren kann.



ICS.LMN.Anwendungsfaelle.40

Der GWH **MUSS** im ICS deklarieren, ob das SMGW den „Master“-Schlüssel gemäß ▶REQ.LMN.Zählerverwaltung.50 aktualisieren kann.

3.3.3. Kommunikationsszenarien

Das SMGW **MUSS** die Anwendungsfälle LAF1 und LAF2 für bidirektional kommunizierende Zähler über LKS1 umsetzen. [REQ.LMN.Kommunikationsszenarien.10] Das SMGW **MUSS** die Registrierung von Zählern und den Anwendungsfall LAF2 für unidirektional kommunizierende Zähler über LKS2 umsetzen. [REQ.LMN.Kommunikationsszenarien.20]

- Bidirektionale Kommunikation
Zugriff des SMGW auf Services des Zählers, um z.B. Messwerte abzufragen oder TLS-Zertifikate einzubringen.
- Unidirektionale Kommunikation
Empfang von Datenpaketen, die Messwerte enthalten, durch das SMGW.

Szenario	Typ	Service Requester	Service Provider
LKS1	BIDIREKTIONAL	SMGW	Zähler
LKS2	UNIDIREKTIONAL	-	Zähler

Tabelle 3.10 Kommunikationsszenarien an der LMN-Schnittstelle

LKS1: BIDIREKTIONAL

Das folgende Diagramm zeigt das Kommunikationsmuster bei bidirektionaler Zählerkommunikation.

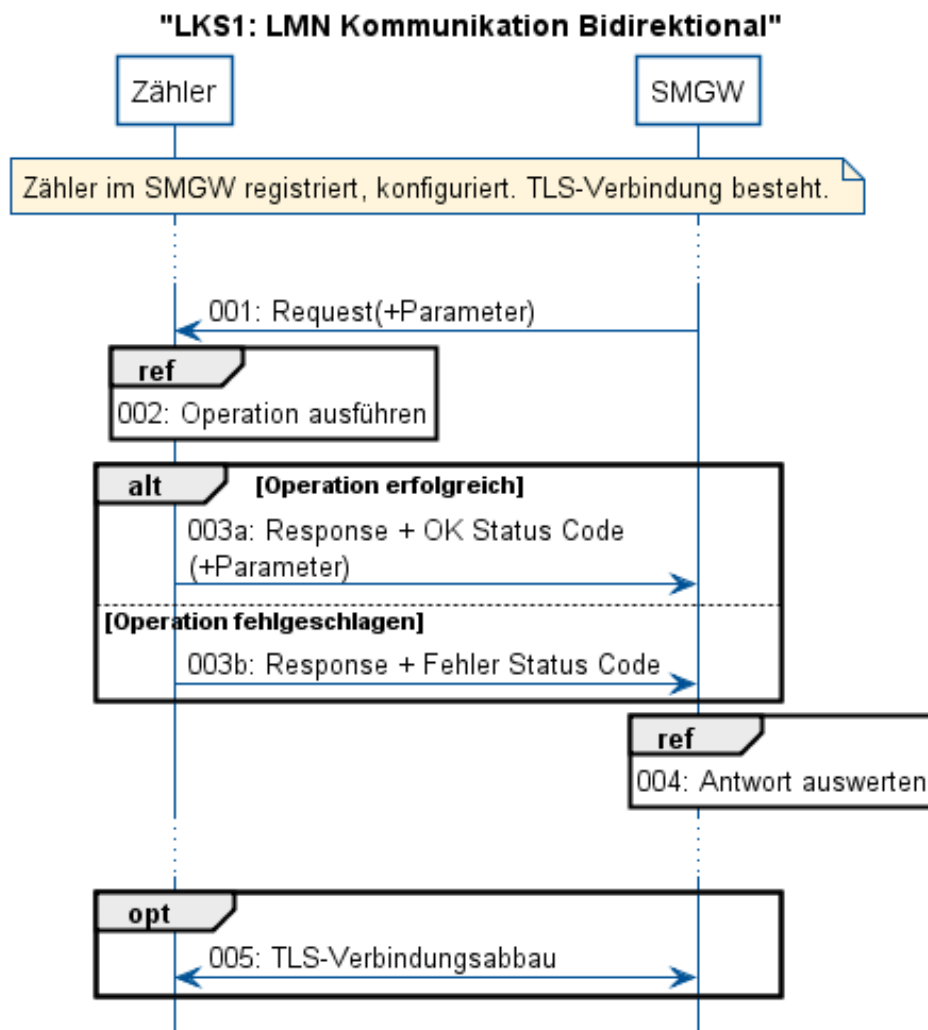


Abbildung 3.10. Sequenzdiagramm für bidirektionale LMN-Kommunikation (LKS1)

Vorbedingung:

Der Zähler ist im SMGW registriert und konfiguriert. Das SMGW kann mit dem Zähler über die TLS-Verbindung kommunizieren.

Rolle des SMGW:

Client

Schritt	Ereignis	Aktivität	Sender	Empfänger	Ausgetauschte Daten
001	-	SMGW erstellt und sendet Anfrage	SMGW	Zähler	Request (+Parameter)
002	Zähler führt die gewünschte Operation aus, z.B. ermittelt die angefragten Messwerte	Zähler führt Anfrage aus	-	-	-
003a	Operation erfolgreich beendet	Zähler sendet Response an SMGW	Zähler	SMGW	Response-Code OK (+Parameter)

Schritt	Ereignis	Aktivität	Sender	Empfänger	Ausgetauschte Daten
003b	Operation nicht erfolgreich beendet	Zähler sendet Response an SMGW	Zähler	SMGW	Response mit Fehler Code
004	SMGW empfängt Zählerantwort	SMGW verarbeitet Antwort	-	-	-

Tabelle 3.11 Beschreibung Kommunikationsszenario LKS1: LMN bidirektional

LKS2: UNIDIREKTIONAL

Das folgende Diagramm zeigt das Kommunikationsmuster bei unidirektionaler Zählerkommunikation.

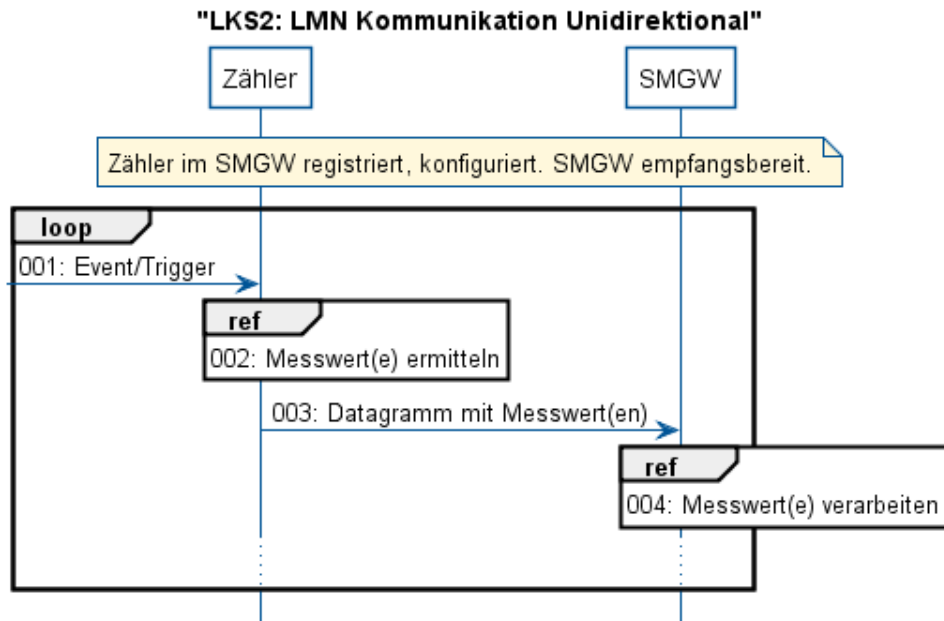


Abbildung 3.11. Sequenzdiagramm für unidirektionale LMN-Kommunikation (LKS2)

Vorbedingung:

Der Zähler ist im SMGW registriert und konfiguriert. Das SMGW ist empfangsbereit, d.h. es kann Pakete vom Zähler empfangen und entschlüsseln.

Rolle des SMGW:

Empfänger

Schritt	Ereignis	Aktivität	Sender	Empfänger	Ausgetauschte Daten
001	Bedingung zur Versendung von Messwerten erfüllt	-	-	-	-
002	-	Der Zähler ermittelt die Messwerte	-	-	-
003	Messwertermittlung erfolgreich und Messwerte gültig	Zähler sendet Datagramm mit Messwerten	Zähler	SMGW	Messwerte

Schritt	Ereignis	Aktivität	Sender	Empfänger	Ausgetauschte Daten
004	SMGW empfängt Messwerte	SMGW verarbeitet Messwerte	-	-	-

Tabelle 3.12 Beschreibung Kommunikationsszenario LKS2: LMN unidirektional

3.3.4. Sicherung der Kommunikationsverbindungen in das LMN

Das SMGW **MUSS** sicherstellen, dass Messwerte, die von Zählern empfangen werden, nur dann akzeptiert werden, wenn sie über eine gesicherte Kommunikation vertraulich, integer und authentisch empfangen wurden. [REQ.LMN.Sicherung.10] Das SMGW gewährleistet diese Anforderung über die in den folgenden Abschnitten beschriebene Sicherung der Kommunikation, die sich für bidirektional und unidirektional kommunizierende Zähler unterscheidet.

Das SMGW **SOLL** dem GWA eine Möglichkeit bereitstellen, ungenutzte physische LMN-Schnittstellen zu deaktivieren und wieder zu reaktivieren. [REQ.LMN.Sicherung.20]

3.3.4.1. Sicherung der LMN-Kommunikation mit TLS

Das SMGW **MUSS** TLS gemäß [TR-03109-3] für die authentische und vertrauliche Kommunikation mit bidirektionalen Zählern im LMN unterstützen. [REQ.LMN.TlsSicherung.10] Das SMGW **MUSS** im LMN die Rolle des TLS-Clients übernehmen können. [REQ.LMN.TlsSicherung.20] Das SMGW **KANN** für optionale zusätzliche LKS im LMN die Rolle des TLS-Servers übernehmen. [REQ.LMN.TlsSicherung.30] Das SMGW **MUSS** beim TLS-Handshake die Dienste des Sicherheitsmodules nutzen (Siehe ▶Abschnitt 5.1.1). [REQ.LMN.TlsSicherung.40]

Zur gegenseitigen Authentifizierung zwischen SMGW und Zählern im LMN **MUSS** das SMGW für die TLS-Kommunikation selbstsignierte X.509 LMN-Zertifikate verwenden. [REQ.LMN.TlsSicherung.50] Das SMGW **MUSS** LMN-Zertifikate nach Detailspezifikation ☞ Zertifikatsprofile am LMN zur Authentifizierung gegenüber Zählern verwenden. [REQ.LMN.TlsSicherung.60] Das SMGW **MUSS** LMN-Zertifikate nach Detailspezifikation ☞ Zertifikatsprofile am LMN für die Zähler erstellen. [REQ.LMN.TlsSicherung.70] Die LMN-Zertifikate (SMGW und Zähler) stammen somit nicht aus der in [TR-03109-4] definierten SM-PKI.



ICS.LMN.TlsSicherung.10

Der GWH **MUSS** im ICS deklarieren, ob das SMGW im LMN die Rolle des TLS-Servers übernehmen kann.

3.3.4.2. Sicherung der LMN-Kommunikation mit symmetrischen Verfahren

Das SMGW **MUSS** die Kommunikation mit unidirektional kommunizierenden Zählern über ein Verfahren basierend auf symmetrischer Kryptografie mit einem zwischen SMGW und Zähler vereinbarten gemeinsamen, geräteindividuellem Schlüssel ("Master-Key") absichern. [REQ.LMN.PskSicherung.10]

Das SMGW **MUSS** die Kommunikation im LMN auf Basis symmetrischer Kryptographie nach [TR-03109-3] für unidirektional kommunizierende Zähler und zur initialen kommunikativen Anbindung bidirektional kommunizierender Zähler verwenden. [REQ.LMN.PskSicherung.20]



ICS.LMN.Sicherung.10

Der GWH **MUSS** im ICS deklarieren, ob das SMGW physische LMN-Schnittstellen deaktivieren und reaktivieren kann und dies im Falle einer Deaktivierbarkeit in einer Anlage zum ICS beschreiben.

3.3.5. Kommunikationsprotokolle

Dieser Abschnitt beschreibt die Anforderungen an das SMGW in Bezug auf die zu unterstützenden Kommunikationsprotokolle im LMN. Prinzipiell wird hier unterschieden zwischen Anforderungen, die auf die Un-

terstützung von Applikationsdatenformaten abzielen, und Anforderungen an das Schnittstellenprotokoll für den Transport der Applikationsdaten.

Die ►Abbildung 3.12 zeigt die Gesamtheit der LMN-Protokollstapel im SMGW. Die Protokollstapel haben abhängig von der physikalischen Schicht unterschiedliche Ausprägungen, die in den nächsten Abschnitten detailliert werden.

Legende

	Pflicht / MUSS	Optional / Offen				
Kommunikationsszenario	Kommunikative Anbindung LKS1	LKS1 Bedrahtet Messdaten SML	LKS2 Drahtlos Messdaten wMBUS	Bidirektional	Kommunikative Anbindung	Unidirektional
Inhaltsdatenmodell	Schlüssel, Zertifikate, Krypto-Parameter (ASN.1)	Messdaten (OBIS), Schlüssel und Zertifikate (ASN.1) (COSEM)	Messdaten (OBIS - MBUS-VIF/DIF)	Messdaten (OBIS) Schlüssel und Zertifikate (ASN.1)	Schlüssel, Zertifikate, Krypto-Parameter (ASN.1)	Messdaten (OBIS)
7: Anwendungsschicht 6: Präsentationsschicht	SYM Nachrichten	SML mit COSEM-Access	Messdatenübertragung MBUS Application Layer	Weitere Protokolle		
5: Sitzungsschicht	N/A		N/A			
Transportsicherung	Authentifizierung & Verschlüsselung mit PSK nach TR-03116-3 Kap.7	SMGW als TLS-Client	MBUS TPL (Verschlüsselung Mode 7) Authentifizierungs-Fragmentierungslayer	SMGW als TLS-Client/ TLS-Server	Authentifizierung und Verschlüsselung mit PSK nach TR-03116-3 Kap.7	
4: Transportschicht 3: Netzwerkschicht 2: Verbindungsschicht	SMGW als HDLC-Master		Wireless MBUS Link-Layer	Bidirektionale Kommunikationsprotokolle		Unidirektionale Kommunikationsprotokolle
1: Physikal. Schicht	EIA/RS 485 (bidirektional)		Wireless MBUS Mode (C), T (unidirektional)			

Abbildung 3.12. Protokollstapel im LMN (für drahtlose und drahtgebundene Kommunikation)

3.3.5.1. Anwendungsprotokolle

Das SMGW **MUSS** die Anwendungsprotokoll-spezifische Codierung der Maßeinheiten und die Identifikation der *Messgrößen* und *Messarten* für elektrische Energie nach [EN62056-6-1] und andere Sparten nach [EN13757-1] mindestens für die in ►Kapitel 4 verwendeten Messgrößen und Messarten umsetzen. [REQ.LMN.Anwendungsprotokolle.10] ¹¹

Das SMGW **MUSS** die Anwendungsprotokoll-spezifische Identifikation der Messeinrichtung in die Identifikation nach [DIN43863-5] umsetzen. [REQ.LMN.Anwendungsprotokolle.20]

Das SMGW **MUSS** die Anwendungsprotokoll-spezifische Codierung von Fehlern, die Integritätsverletzungen an der Messeinrichtung, ungültige Messwerte oder zu geringe Versorgungsspannungen anzeigen, der Messwertverarbeitung des SMGW mitteilen. [REQ.LMN.Anwendungsprotokolle.30]

3.3.5.2. Kommunikationsprotokolle

Das SMGW **MUSS** im LMN mindestens eine drahtlose und eine drahtgebundene Schnittstelle zur Verfügung stellen. [REQ.LMN.Kommunikationsprotokolle.10]

3.3.5.2.1. Drahtlose Schnittstelle

Das SMGW **MUSS** die unidirektionale, drahtlose Kommunikation im LMN (LKS2) mit einem Wireless M-Bus Protokollstapel gemäß den Anforderungen der Detailspezifikation ↗ Detailspezifikation Wireless MBUS unterstützen. [REQ.LMN.Kommunikationsprotokolle.20]

Das SMGW **MUSS** die Messwerte und Statusinformationen der M-Bus Anwendungsschicht nach Spezifikation [EN13757-3] verarbeiten und die *Messgrößen* und *Messarten* nach OBIS-Kennzahlen gemäß [EN13757-1], [EN62056-6-1] und [OMSS4] Annex A identifizieren. [REQ.LMN.Kommunikationsprotokolle.30]

¹¹ Die für die Messwertverarbeitung im SMGW zulässigen OBIS-Kennzahlen werden über das Regelwerk der Tarifierungsanforderungen bestimmt.

3.3.5.2.2. Drahtgebundene Schnittstelle

Das SMGW **MUSS** die bidirektionale, drahtgebundene Kommunikation im LMN (LKS1) mit einem Protokollstapel COSEM/OBIS - SML - TLS - HDLC - RS485 gemäß der Anforderungen [VDE0418-63-9] und Detailspezifikation ☞ Bidirektionale LMN-Kommunikation über HDLC unterstützen. [REQ.LMN.Kommunikationsprotokolle.40]

Das SMGW **MUSS** die Messwerte und Statusinformationen der Anwendungsschicht nach Spezifikation [VDE0418-63-9] verarbeiten und die *Messgrößen* und *Messarten* nach OBIS-Kennzahlen gemäß [EN13757-1] und [EN62056-6-1] identifizieren. [REQ.LMN.Kommunikationsprotokolle.50]

3.4. Vorgaben an die Kommunikationsverbindungen in das HAN

3.4.1. Übersicht

Im Folgenden werden die Vorgaben an die Kommunikation zwischen den Teilnehmern im HAN und dem SMGW beschrieben. Anwendungsfälle, die eine HAN-Kommunikation erfordern, werden in ▶Abschnitt 3.4.2 skizziert. Zur Realisierung dieser Anwendungsfälle werden mehrere Kommunikationsszenarien herangezogen, welche vom SMGW unterstützt werden müssen. Diese werden in ▶Abschnitt 3.4.3 definiert. Die Anforderungen an die Sicherung der Kommunikationsverbindungen werden in ▶Abschnitt 3.4.4 formuliert. In ▶Abschnitt 3.4.6 werden die technischen Anforderungen an die HAN-Schnittstelle dargelegt, während ▶Abschnitt 3.4.5 die notwendigen Parameter zur Kommunikation beschreibt.

3.4.2. Anwendungsfälle an der HAN-Schnittstelle

Dieser Abschnitt beschreibt diejenigen Anwendungsfälle (gekennzeichnet mit dem Kürzel HAF), die eine Kommunikation des SMGW mit Teilnehmern im HAN erfordern. Zusätzlich werden die Anwendungsfälle beschrieben, die einen transparenten Kanal durch das SMGW zwischen CLS im HAN und aktivem EMT im WAN erfordern.

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

1. Bereitstellung von Daten für den Anschlussnutzer.
2. Bereitstellung von Daten für den Servicetechniker.
3. Transparenter Kommunikationskanal zwischen CLS und aktivem EMT.
4. Herstellen der GWA-Kommunikation durch den Servicetechniker
5. Das Auslösen von Selbsttest-Funktionen durch den Servicetechniker

Das SMGW **KANN** weitere Anwendungsfälle am HAN unterstützen. [REQ.HAN.Anwendungsfaelle.10]

3.4.2.1. HAF1: Bereitstellung von Daten für den Anschlussnutzer

"Das SMGW bietet eine Schnittstelle im HAN an, über die das SMGW dem berechtigten Anschlussnutzer seine Messwerte und andere für ihn relevante Informationen bereitstellt, um sie beispielsweise über eine Anzeigeeinheit zur Rechnungsprüfung zu visualisieren. Als Anzeigeeinheit kann zur Rechnungsprüfung ein Gerät mit Transparenz- und Display-Software nach [MessEG]/[MessEV] verwendet werden.

Unter Verwendung des Anwendungsfalls HAF1 kann somit die Bereitstellung von abrechnungsrelevanten Daten und von *aktuellen Werten* sowie die zugehörigen Tarifinformationen gemäß den Anwendungsfällen der Tarifierung aus ▶Kapitel 4 gewährleistet werden. Ebenso ermöglicht der Anwendungsfall HAF1 die Bereitstellung von historischen Energieverbrauchs- oder Einspeisedaten.

Zusätzlich wird mithilfe dieses Anwendungsfalls die Bereitstellung der Daten aus dem Anschlussnutzer-Log gewährleistet.

Das SMGW stellt mindestens folgende Informationen an der Schnittstelle bereit:

- Das SMGW **MUSS** alle Daten des Anschlussnutzer-Logs gemäß ▶Abschnitt 5.3.2 bereitstellen. [REQ.HAN.AnschlussnutzerDatenbereitstellung.10]
- Das SMGW **MUSS** die mit der gesetzlichen Zeit synchronisierte Systemzeit und das Datum (Stunden, Minuten, Sekunden, Tag, Monat, Jahr) bereitstellen. [REQ.HAN.AnschlussnutzerDatenbereitstellung.20]
- Das SMGW **MUSS** dem Anschlussnutzer an der HAN-Schnittstelle die Identifikation der Software-Version des SMGW bereitstellen. [REQ.HAN.AnschlussnutzerDatenbereitstellung.30] ¹²
- Das SMGW **MUSS** die letzten im SMGW registrierten Zählerstände in einer verkehrsgebräuchlichen Einheit (kWh, kVar, m³) der am SMGW angeschlossenen und dem Anschlussnutzer zugeordneten Zähler, die Zähler-Identifikation sowie die OBIS-Kennzahl und den Fehlerstatus der Messwerte bereitstellen. [REQ.HAN.AnschlussnutzerDatenbereitstellung.40]
- Das SMGW **SOLL** - gemäß des durch den GWA parametrisierten Zählerabfrage- und Messwernerfassungsintervalls - den letzten vom SMGW authentisch empfangenen *Zählerstand* bereitstellen. [REQ.HAN.AnschlussnutzerDatenbereitstellung.50]
- Das SMGW **MUSS** Zählerstände für elektrische Energie für mindestens die letzten 3 Jahre oder für den Zeitraum seit Beginn des Gültigkeitszeitraums des jeweiligen Auswertungsprofils (falls dieser kürzer ist) für den Anschlussnutzer (ggf. über die Transparenz- und Displaysoftware TRuDI) bereitstellen, die den Abrechnungsperioden entsprechen. [REQ.HAN.AnschlussnutzerDatenbereitstellung.60]
- Das SMGW **MUSS** Zählerstände für elektrische Energie für die letzten 24 Monate für den Anschlussnutzer bereitstellen, so dass der Anschlussnutzer (ggf. über die Transparenz- und Displaysoftware TRuDI) daraus historische tages-, wochen-, monats- und jahresbezogene Energieverbrauchs- oder Einspeisewerte bestimmen kann. [REQ.HAN.AnschlussnutzerDatenbereitstellung.70]
- Das SMGW **MUSS** die Identifikation der dem Anschlussnutzer zugeordneten Tarifierungsfälle und die für den jeweiligen Anschlussnutzer zu visualisierenden Daten (siehe normative Abschnitte des ▶Kapitel 4) bereitstellen. [REQ.HAN.AnschlussnutzerDatenbereitstellung.80]
- Das SMGW **MUSS** die registrierten Zählerstände, mit der für den jeweiligen abrechnungsrelevanten Tarif erforderlichen Registrierperiode nach eichrechtlichen Vorgaben mindestens für die letzten 15 Monate bereitstellen. [REQ.HAN.AnschlussnutzerDatenbereitstellung.90]
- Das SMGW **MUSS** dem Anschlussnutzer an der HAN-Schnittstelle die *Anschlussnutzerkennung* des Regelwerkes der Messwertverarbeitung bereitstellen, sofern diese Kennung nicht dem Benutzernamen für die Authentifizierung entspricht. [REQ.HAN.AnschlussnutzerDatenbereitstellung.100]
- Das SMGW **MUSS** dem Anschlussnutzer an der HAN-Schnittstelle die in den normativen Tarifierungsfällen des ▶Kapitel 4 genannten Informationen für den Anschlussnutzer bereitstellen. [REQ.HAN.AnschlussnutzerDatenbereitstellung.110]
- Das SMGW **SOLL** dem Anschlussnutzer an der HAN-Schnittstelle die Möglichkeit bieten, anhand der SMGW-ID die Kommunikationsadressen (IP-Adresse, Portnummer, URI) herauszufinden, mit denen er auf die für ihn bereitgestellten Informationen zugreifen kann. [REQ.HAN.AnschlussnutzerDatenbereitstellung.120]



ICS.HAN.AnschlussnutzerDatenbereitstellung.10

Der GWH **MUSS** im ICS beschreiben, ob das SMGW die Identifikation der Kommunikationsadressen und URLs für den Anschlussnutzer ermöglicht und in einer Anlage zum ICS beschreiben, über welche Kommunikationsadresse, welches Zugriffsprotokoll, welche Transfersyntax und welche Datenstrukturen der Anschlussnutzer auf die vom SMGW bereitgestellten Daten im HAN zugreifen kann.

¹² Sofern mehrere Software-Teile identifizierbar sind, die Teile der Software, die nach [MessEG] und [MsbG] relevant sind.



ICS.HAN.AnschlussnutzerDatenbereitstellung.20

Der GWH **MUSS** im ICS beschreiben, ob das SMGW den zuletzt authentisch empfangenen Zählerstand gemäß ▶REQ.HAN.AnschlussnutzerDatenbereitstellung.50 bereitstellen kann.

3.4.2.2. HAF2: Bereitstellung von Daten für den Servicetechniker

Anwendungsfall HAF2 ermöglicht die Bereitstellung von Informationen aus dem System-Log sowie weitere herstellerspezifische Diagnose-Informationen für den Servicetechniker.

Das SMGW stellt dem Servicetechniker folgende Informationen bereit:

- Das SMGW **MUSS** alle Daten des System-Logs bereitstellen. [REQ.HAN.ServiceTechnikerDatenbereitstellung.10]
- Das SMGW **KANN** weitere Konfigurations- und Statusinformationen zur Diagnose von Kommunikationsfehlern bereitstellen. [REQ.HAN.ServiceTechnikerDatenbereitstellung.20]

Beispielsweise:

- Konfigurationsparameter der Schnittstellen im WAN, HAN und LMN
 - Kommunikationsprofile
 - Zählerprofile
 - Proxy-Kommunikationsprofile
- Statusinformationen der Schnittstellen im WAN, HAN und LMN
- Liste und Statusinformationen der Sensoren
- Liste und Statusinformationen der CLS-Schnittstellen
- Statusinformationen des SMGW
- Netzwerk-Diagnoseinformationen der WAN-Schnittstelle

Das SMGW **SOLL** dem Servicetechniker an der HAN-Schnittstelle die Möglichkeit bieten, anhand der SMGW-ID die Kommunikationsadressen (IP-Adresse, Portnummer, URI) herauszufinden, mit denen er auf die für ihn bereitgestellten Informationen zugreifen kann. [REQ.HAN.ServiceTechnikerDatenbereitstellung.30]



ICS.HAN.ServiceTechnikerDatenbereitstellung.10

Der GWH **MUSS** im ICS beschreiben, ob der Servicetechniker auf mehr als das System-Log zugreifen kann und in einer Anlage zum ICS beschreiben auf welche Daten der Servicetechniker zugreifen kann und über welche Kommunikationsadressen, mit welchen Protokollen, welcher Transfer-syntax und welchen Datenstrukturen dies geschieht.



ICS.HAN.ServiceTechnikerDatenbereitstellung.20

Der GWH **MUSS** im ICS beschreiben, ob das SMGW die Identifikation der Kommunikationsadressen und URLs für den Servicetechniker anhand der SMGW-ID ermöglicht und in einer Anlage zum ICS beschreiben, über welche Kommunikationsadresse, welches Zugriffsprotokoll, welche Transfer-syntax und welche Datenstrukturen der Servicetechniker auf die vom SMGW bereitgestellten Daten zugreifen kann.

3.4.2.3. HAF3: Transparenter Kommunikationskanal zwischen CLS und aktivem EMT

Der Anwendungsfall HAF3 ermöglicht es CLS im HAN über das SMGW mit autorisierten aktivem EMT im WAN zu kommunizieren.

Das SMGW **MUSS** eine Proxy-Funktionalität besitzen, um einen transparenten Kommunikationskanal zwischen berechtigtem EMT im WAN und berechtigtem CLS im HAN bereitzustellen. [REQ.HAN.Transparenter-Kanal.10]

Für den Fall, dass ein Kanal von einem aktivem EMT an ein CLS aufgebaut werden soll, erfolgt die Initiierung über den GWA, da ein aktiver EMT keine direkte Verbindung zum SMGW aufbauen kann. Dazu sendet der GWA einen entsprechenden Administrationsbefehl an das SMGW.

Ebenso ermöglicht der Anwendungsfall HAF3 den Aufbau eines transparenten Kanals zwischen einem CLS und einem aktiven EMT, der durch das SMGW aufgrund von konfigurierten Parametern oder durch das CLS initiiert wird.

3.4.2.4. HAF4: Herstellen der GWA-Kommunikation durch den Servicetechniker

Anwendungsfall HAF4 ermöglicht dem Servicetechniker die Wiederherstellung der WAN-Kommunikationsfähigkeit zum GWA, indem er über die HAN-Schnittstelle Kommunikationsparameter ändert, die nach [PP-0073] nicht die Sicherheitsfunktion des SMGW beeinflussen.

Das SMGW **KANN** dem Servicetechniker ermöglichen, die Verbindungsadresse (IP-Adresse, Port-Nummer) zur Herstellung der WAN-Kommunikation mit dem GWA-System (Management, Zeitserver) zu ändern. [REQ.HAN.ServiceTechnikerGwaKommunikation.10]

Das SMGW **KANN** dem Servicetechniker ermöglichen, die Konfigurationsparameter der physischen WAN-Schnittstelle zur Anmeldung an das WAN-Zugangsnetz zu ändern (SIM-PIN, den Access-Point-Name oder die Access-Point-Credentials). [REQ.HAN.ServiceTechnikerGwaKommunikation.20]

Das SMGW **KANN** dem Servicetechniker ermöglichen, die zuvor vom GWA konfigurierten WAN-Zugangsnetzparameter zu aktivieren. [REQ.HAN.ServiceTechnikerGwaKommunikation.30]



ICS.HAN.ServiceTechnikerGwaKommunikation.10

Der GWH **MUSS** im ICS deklarieren, ob das SMGW den ▶HAF4: Herstellen der GWA-Kommunikation durch den Servicetechniker unterstützt und in einer Anlage zum ICS beschreiben, welche Konfigurationsparameter der Servicetechniker auf welche Weise ändern kann.

3.4.2.5. HAF5: Auslösen von Selbsttest-Funktionen

Anwendungsfall HAF5 ermöglicht dem Servicetechniker das Auslösen von Selbsttest-Funktionen gemäß [PP-0073] und [MessEG]/[MessEV].

Das SMGW **SOLL** dem Servicetechniker ermöglichen, Selbsttests gemäß ▶Abschnitt 3.2.9 über die HAN-Schnittstelle zu starten. [REQ.HAN.ServiceTechnikerSelbsttest.10]

Das SMGW **MUSS** das Auslösen eines Selbsttestes durch den Servicetechniker und das Ergebnis des Selbsttestes im System-Log protokollieren und bei Ergebnissen, die nach [MessEG]/[MessEV] relevant sind im Eichlog protokollieren und den GWA benachrichtigen. [REQ.HAN.ServiceTechnikerSelbsttest.20]



ICS.HAN.ServiceTechnikerSelbsttest.10

Der GWH **MUSS** im ICS deklarieren, ob das SMGW den ▶HAF5: Auslösen von Selbsttest-Funktionen unterstützt und in diesem Fall in einer Anlage zum ICS beschreiben, wie der Servicetechniker Selbsttests starten kann.

3.4.3. Kommunikationsszenarien

Das SMGW **MUSS** die notwendige Kommunikation mit Teilnehmern im HAN der in ▶Abschnitt 3.4.2 skizzierten Anwendungsfälle HAF1 bis HAF5 über jeweils eines der Kommunikationsszenarien HKS1-HKS5 umsetzen. [REQ.HAN.Kommunikationsszenarien.10]

Die folgenden Abschnitte beschreiben die Kommunikationsszenarien der HAN-Schnittstelle des SMGW:

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

Das SMGW **MUSS** die Kommunikationsszenarien HKS1 bis HKS3 umsetzen. [REQ.HAN.Kommunikationsszenarien.20]

Das SMGW **MUSS** mindestens eines der Kommunikationsszenarien HKS4 und HKS5 umsetzen. [REQ.HAN.Kommunikationsszenarien.30]

Szenario	TLS-Client	TLS-Server	Client Authentifizierung	Server-Authentifizierung
HKS1	Anschlussnutzer	SMGW	CON_HAN_TLS_CERT	GW_HAN_TLS_CERT
HKS1	Servicetechniker	SMGW	SRV_HAN_TLS_CERT	GW_HAN_TLS_CERT
HKS2	Anschlussnutzer	SMGW	Digest-Authentifizierung	GW_HAN_TLS_CERT
HKS3	CLS	SMGW	CLS_HAN_TLS_CERT	GW_HAN_TLS_CERT
HKS4	SMGW	CLS	GW_HAN_TLS_CERT	CLS_HAN_TLS_CERT
HKS5	SMGW	CLS	GW_HAN_TLS_CERT	CLS_HAN_TLS_CERT

Tabelle 3.13 Kommunikationsszenarien an der HAN-Schnittstelle

Die Kommunikationsszenarien HKS1 bis HKS5 unterscheiden sich in der Art und Weise der Authentifizierung des Teilnehmers im HAN (Anschlussnutzer/Servicetechniker) sowie der Initiierung des transparenten Kommunikationskanals. In allen Kommunikationsszenarien erfolgt die Kommunikation bidirektional.

Im Folgenden werden diese Kommunikationsszenarien beschrieben.

3.4.3.1. Kommunikationsszenario HKS1: Webservices des SMGW mit Client-Authentifizierung durch HAN-Zertifikate

Beim Aufbau der TLS-Verbindung zwischen dem Teilnehmer im HAN und dem SMGW wird im TLS-Handshake mittels der Zertifikate *GW_HAN_TLS_CERT* und *CON_HAN_TLS_CERT* bzw. *SRV_HAN_TLS_CERT* und deren zugehörigen Schlüsseln eine Client-Server Authentifizierung durchgeführt. Das Zertifikat *CON_HAN_TLS_CERT* bzw. *SRV_HAN_TLS_CERT* ist dabei eindeutig einem dem SMGW bekannten Anschlussnutzer bzw. Servicetechniker zugeordnet.

Rolle des SMGW:

TLS-Server, Webservice-Server

Akteur	Beschreibung
SMGW	<p>Das SMGW MUSS als TLS-Server fungieren, über ein eindeutiges HAN-Zertifikat <i>GW_HAN_TLS_CERT</i> verfügen und das Schlüsselmaterial zum HAN-Zertifikat im Sicherheitsmodul speichern. [REQ.HAN.HKS1.10]</p> <p>Dieses Zertifikat wird von der HAN-Komponente des Anschlussnutzers oder Servicetechnikers zum Aufbau der TLS-Verbindung genutzt und kann verwendet werden um das SMGW zu authentifizieren.</p>

Akteur	Beschreibung
Anschlussnutzer/ Servicetechniker	Das SMGW MUSS die HAN-Komponente des Anschlussnutzers oder Servicetechnikers über ein Zertifikat CON_HAN_TLS_CERT bzw. SRV_HAN_TLS_CERT authentifizieren. [REQ.HAN.HKS1.20]

Tabelle 3.14 HKS1: Authentifizierung des Anschlussnutzers/Servicetechnikers mittels HAN-TLS-Client-Zertifikat



Abbildung 3.13. Authentifizierung des Anschlussnutzers/Servicetechnikers mittels HAN-TLS-Client-Zertifikat

Nach erfolgreicher Authentifizierung muss das SMGW Ergebnisse zu den vom Anschlussnutzer bzw. Servicetechniker abgesetzten Datenabfragen gemäß den Anwendungsfällen HAF1 bzw. HAF2 liefern. Es werden nur Daten übermittelt, die dem authentifizierten Anschlussnutzer bzw. Servicetechniker zugeordnet sind.

Umzusetzende Anwendungsfälle

Das SMGW **MUSS** die Kommunikation mit dem Anschlussnutzer für den Anwendungsfall HAF1 über das Kommunikationsszenario HKS1 unterstützen. [REQ.HAN.HKS1.30]

Das SMGW **MUSS** die Kommunikation mit dem Servicetechniker für den Anwendungsfall HAF2 und HAF4 über das Kommunikationsszenario HKS1 unterstützen. [REQ.HAN.HKS1.40]

3.4.3.2. Kommunikationsszenario HKS2: Webservices des SMGW mit Client-Authentifizierung durch Kennung und Passwort

In diesem Fall übernimmt das SMGW die TLS-Server-Rolle und der Anschlussnutzer nimmt mithilfe einer Anzeigeeinheit die TLS-Client-Rolle ein. Ein Servicetechniker darf das Kommunikationsszenario HKS2 nicht verwenden.

Beim Aufbau der TLS-Verbindung zwischen Anschlussnutzer und dem SMGW wird im TLS-Handshake mittels des Zertifikats GW_HAN_TLS_CERT eine Server Authentifizierung durchgeführt. Anschließend werden mittels einer HTTP-Digest-Access-Authentication Kennung und Passwort abgefragt und diese Credentials an das SMGW übermittelt. Das SMGW **MUSS** sicherstellen, dass die dem Anschlussnutzer zugeordnete Kennung im SMGW eindeutig ist. [REQ.HAN.HKS2.10]

Rolle des SMGW:

TLS-Server, Webservice-Server

Akteur	Beschreibung
SMGW	Das SMGW MUSS als TLS-Server fungieren, über ein eindeutiges HAN-Zertifikat GW_HAN_TLS_CERT verfügen und das Schlüsselmaterial zum HAN-Zertifikat im Sicherheitsmodul speichern. [REQ.HAN.HKS2.20] Dieses Zertifikat wird von der HAN-Komponente des Anschlussnutzers zum Aufbau der TLS-Verbindung genutzt und kann verwendet werden um das SMGW zu authentifizieren.

Akteur	Beschreibung
Anschlussnutzer	Das SMGW MUSS den Anschlussnutzer über eine eindeutige Kennung und Passwort mittels HTTP-Digest-Authentication innerhalb einer TLS-Verbindung authentifizieren. [REQ.HAN.HKS2.30]

Tabelle 3.15 HKS2: Authentifizierung des Anschlussnutzers mittels Kennung und Passwort

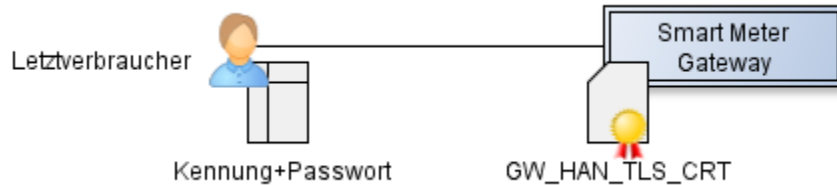


Abbildung 3.14. Authentifizierung des Anschlussnutzers mittels Kennung und Passwort

Nach erfolgreicher beidseitiger Authentifizierung darf das SMGW Ergebnisse zu den vom Anschlussnutzer abgesetzten Datenabfragen gemäß dem Anwendungsfall HAF1 liefern. Es werden nur Daten übermittelt, die dem authentifizierten Anschlussnutzer zugeordnet sind.

Umzusetzende Anwendungsfälle

Das SMGW **MUSS** die Kommunikation mit dem Anschlussnutzer für den Anwendungsfall HAF1 über das Kommunikationsszenario HKS2 unterstützen. [REQ.HAN.HKS2.40]

3.4.3.3. Kommunikationsszenario HKS3: Transparenter Kommunikationskanal initiiert durch CLS

Beschreibung

Beim Aufbau einer TLS-Verbindung vom CLS zum SMGW an die zuvor vereinbarte Kommunikationsadresse übermittelt das CLS dem SMGW authentisch die Identifikation des aktiven EMT, zu dem eine TLS-Proxy-Verbindung hergestellt werden soll.

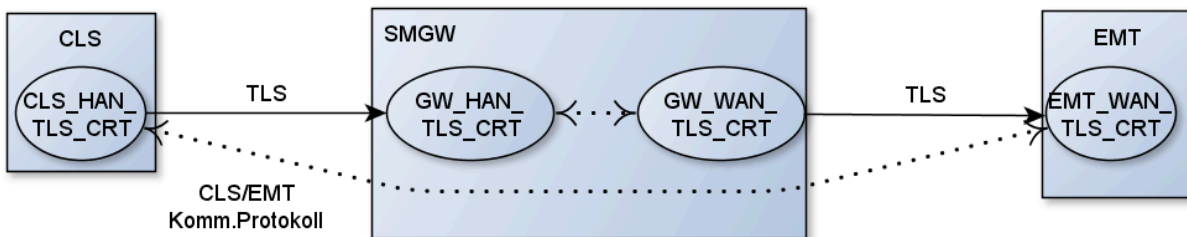


Abbildung 3.15. Transparenter Kommunikationskanal initiiert durch CLS

Notwendige Vorbedingungen

Akteur	Beschreibung
SMGW	<p>SMGW-WAN:</p> <p>Das SMGW MUSS das WAN Kommunikationsszenario TLS-PROXY (Siehe ▶Abschnitt 3.2.3.6) für die Kommunikation mit dem aktiven EMT verwenden. [REQ.HAN.HKS3.10]</p> <p>SMGW-HAN:</p> <p>Das SMGW MUSS als TLS-Server fungieren, über ein geräteindividuelles HAN-Zertifikat GW_HAN_TLS_CERT verfügen und das Schlüsselmaterial zum HAN-Zertifikat im Sicherheitsmodul speichern. [REQ.HAN.HKS3.20]</p> <p>Dieses Zertifikat wird vom CLS zum Aufbau der TLS-Verbindung genutzt und kann verwendet werden um das SMGW zu authentifizieren.</p> <p>Das SMGW MUSS über ein Steuerungsprotokoll die Identifikation des Proxy-Kommunikationsprofils empfangen können, das verwendet wird, um zu einem aktiven EMT einen Proxy-Kanal aufzubauen. [REQ.HAN.HKS3.30]</p> <p>Die Zulässigkeit der Proxy-Verbindung und die Kommunikationsparameter für den Verbindungsaufbau zum aktiven EMT sind in dem identifizieren Proxy-Kommunikationsprofil konfiguriert.</p> <p>Das SMGW MUSS prüfen, dass die im Verbindungsaufbau authentisch empfangene Identifikation eindeutig ein Proxy-Kommunikationsprofil (siehe ▶Abschnitt 3.4.5.3) identifiziert (über die EMT-ID oder Identifikation des Proxy-Kommunikationsprofils). [REQ.HAN.HKS3.40]</p>
CLS	<p>Das CLS agiert als TLS-Client, übermittelt im TLS-Verbindungsaufbau die Identifikation des aktiven EMT und verfügt über ein geräteindividuelles HAN-Zertifikat CLS_HAN_TLS_CERT.</p> <p>Dieses Zertifikat MUSS vom SMGW genutzt werden, um das CLS zu authentifizieren. [REQ.HAN.HKS3.50]</p>
EMT	<p>Der aktive EMT agiert als TLS-Server und verfügt über ein eindeutiges WAN-Zertifikat EMT_WAN_TLS_CERT. Dieses Zertifikat MUSS vom SMGW genutzt werden, um den EMT zu authentifizieren. [REQ.HAN.HKS3.60]</p> <p>Für den aktiven EMT ist im SMGW ein eindeutiger Bezeichner konfiguriert, welcher zur Adressierung des aktiven EMT benutzt werden kann.</p>

Tabelle 3.16 HKS3: Transparenter Kommunikationskanal initiiert durch CLS

Umzusetzende Anwendungsfälle

Das SMGW **MUSS** die Kommunikation mit dem CLS für den Anwendungsfall HAF3 über das Kommunikationsszenario HKS3 unterstützen. [REQ.HAN.HKS3.70]

Weitere Anforderungen

Das SMGW **SOLL** die Identifikation des Proxy-Kommunikationsprofils aus dem Steuerungsprotokoll gemäß Detailspezifikation ☞ Proxy-Signalisierung mit SOCKS entnehmen können. [REQ.HAN.HKS3.80]

Das SMGW **KANN** die Identifikation des Proxy-Kommunikationsprofils aus der TLS-Servername-Indication gemäß Detailspezifikation ☞ Proxy-Signalisierung mit TLS Servername-Indication entnehmen. [REQ.HAN.HKS3.90]



ICS.HAN.HKS3.10

Der GWH **MUSS** im ICS deklarieren, ob das SMGW die Proxy-Signalisierung gemäß Detailspezifikation Proxy-Signalisierung mit SOCKS zur Identifikation des für den Verbindungsaufbau zu verwendenden Proxy-Kommunikationsprofils unterstützt.



ICS.HAN.HKS3.20

Der GWH **MUSS** im ICS deklarieren, ob das SMGW die Proxy-Signalisierung gemäß Detailspezifikation Proxy-Signalisierung mit TLS Servername-Indication zur Identifikation des für den Verbindungsaufbau zu verwendenden Proxy-Kommunikationsprofils unterstützt.

3.4.3.4. Kommunikationsszenario HKS4: Transparenter Kommunikationskanal initiiert durch aktiven EMT

Beschreibung

Dieses Szenario beschreibt den Fall, dass ein aktiver EMT einen transparenten Kommunikationskanal mit einem CLS benötigt. Dazu ist es notwendig, dass der GWA die benötigten TLS-Verbindungen zum aktiven EMT und CLS initiiert.

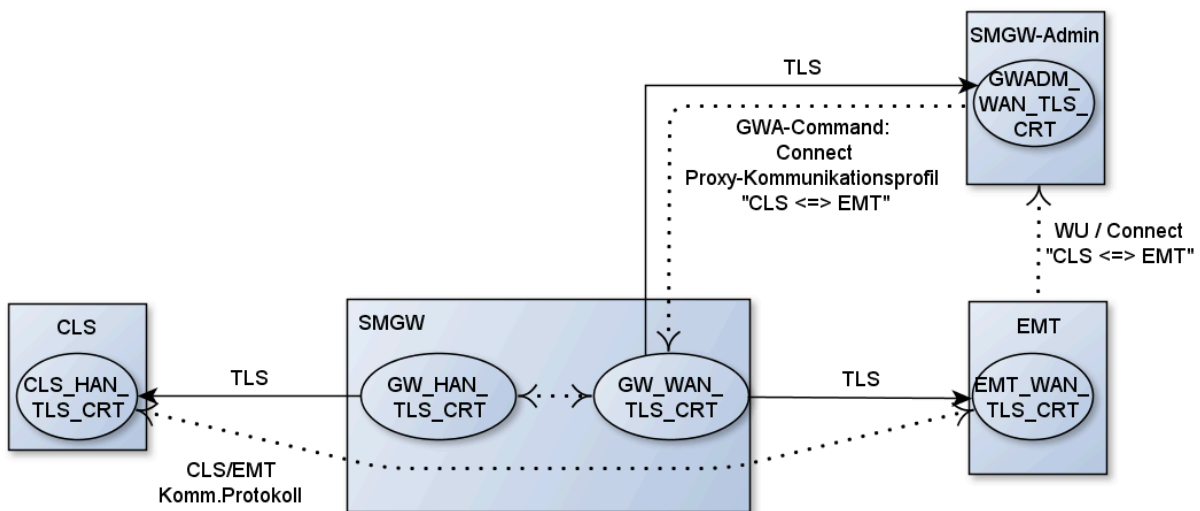


Abbildung 3.16. Transparenter Kommunikationskanal initiiert durch aktiven EMT (über den GWA)

Im Folgenden werden die notwendigen Prozessschritte genauer betrachtet.

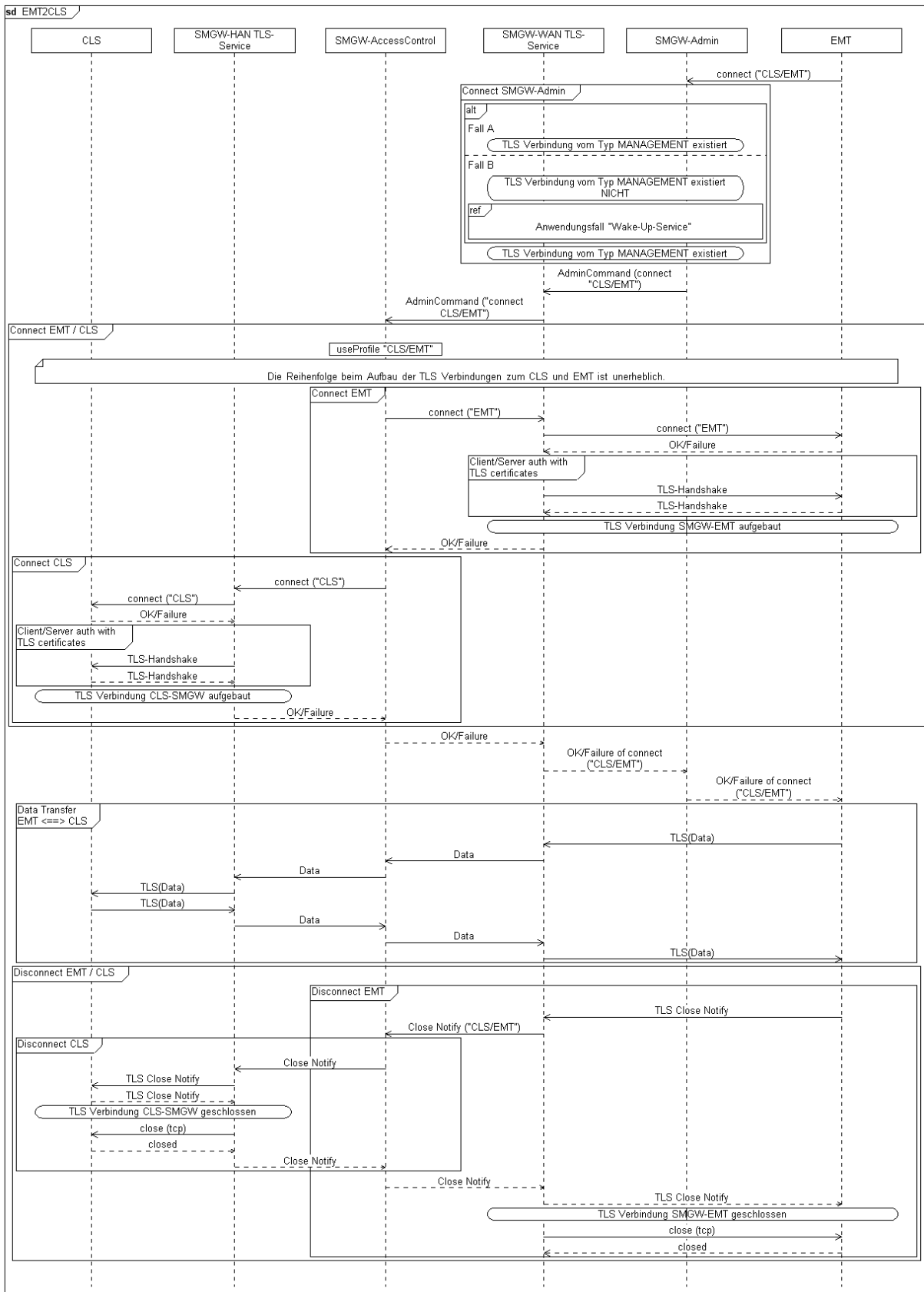


Abbildung 3.17. Sequenzdiagramm Transparenter Kommunikationskanal initiiert durch aktiven EMT

Die Ablaufreihenfolge des Sequenzdiagrammes ist beispielhaft. Es ist sinnvoll zunächst die Verbindung vom SMGW zum CLS aufzubauen und im Erfolgsfall die WAN-Verbindung vom SMGW zum aktiven EMT. Der TLS-Verbindungsabbau kann sowohl vom SMGW, vom CLS oder vom aktiven EMT initiiert werden. Das SMGW terminiert dann die jeweils andere zum Proxy-Kommunikationskanal gehörende TLS-Verbindung.

Ablaufbeschreibung:

- a. Der aktive EMT teilt die gewünschte Zieladresse des CLS dem GWA (z.B. über einen Webservice) mit. Die Schnittstelle aktiver EMT - GWA wird nicht durch diese TR festgelegt.
- b. (Optional) Der GWA schickt ein Wake-Up-Paket zum SMGW, damit dieses die TLS-Verbindung vom Typ „MANAGEMENT“ zum GWA aufbaut.
- c. Der GWA sendet über die bestehende TLS-Verbindung den Administrationsbefehl zum SMGW, der direkt oder über das Tupel (EMT-ID, CLS-ID) das Proxy-Kommunikationsprofil identifiziert, das die Kommunikationsparameter für den Proxy-Kanal enthält.
- d. Auf dem SMGW ist im Proxy-Kommunikationsprofil der aktive EMT als zulässiger Kommunikationspartner für dieses CLS eingetragen.
- e. Aufbau der HAN-TLS-Verbindung vom SMGW zum CLS:
 - i. TLS Client-Server Identifikation und Authentifizierung mit Hilfe der Zertifikate des SMGW im HAN und des CLS-Zertifikats.
 - ii. Protokollierung des Ergebnisses des HAN-Verbindungsaufbaus im System-Log.
- f. Aufbau der WAN-TLS-Verbindung vom SMGW zum aktiven EMT:
 - i. TLS Client-Server Identifikation und Authentifizierung mit Hilfe der Zertifikate von SMGW im WAN und des aktiven EMT Zertifikats.
 - ii. Protokollierung des Ergebnisses des WAN-Verbindungsaufbaus im System-Log.
- g. SMGW meldet Connect-Response (Status OK oder Fehler) des Aufbaus der TLS-Verbindungen an den GWA.
- h. (Optional) GWA meldet den Connect-Response an den aktiven EMT (z.B. durch einen Webservice). Alternativ kann der erfolgreiche TLS-Verbindungsaufbau beim aktiven EMT als „OK“ gewertet werden.
- i. Transparente Datenkommunikation über die beiden etablierten TLS-Verbindungen.
- j. Beenden der TLS-Verbindungen.

Notwendige Vorbedingungen

Akteur	Beschreibung
SMGW	<p>SMGW-WAN:</p> <p>Das SMGW MUSS das WAN Kommunikationsszenario TLS-PROXY (Siehe ▶Abschnitt 3.2.3.6) für die Kommunikation mit dem aktiven EMT verwenden. [REQ.HAN.HKS4.10]</p> <p>SMGW-HAN:</p> <p>Das SMGW MUSS im HKS4 als TLS-Client fungieren, über ein geräteindividuelles HAN-Zertifikat GW_HAN_TLS_CERT verfügen und das Schlüsselmaterial zum HAN-Zertifikat im Sicherheitsmodul speichern. [REQ.HAN.HKS4.20]</p> <p>Dieses Zertifikat wird vom CLS zum Aufbau der TLS-Verbindung genutzt und kann verwendet werden um das SMGW zu authentifizieren.</p> <p>Proxy-Kommunikationsprofil:</p> <p>Das SMGW MUSS prüfen, dass der Administrationsbefehl direkt über ein Tupel (CLS-ID, EMT-ID) ein Proxy-Kommunikationsprofil (siehe ▶Abschnitt 3.4.5.3) im SMGW identifiziert. [REQ.HAN.HKS4.30]</p>
GWA	<p>Der GWA agiert als TLS-Server und verfügt über ein eindeutiges WAN-Zertifikat GWADM_WAN_TLS_CERT</p> <p>Der GWA kann ein Wake-Up-Paket für das SMGW erstellen und kennt die Kommunikationsparameter zur Zustellung dieses Pakets beim SMGW.</p>
CLS	<p>Das CLS agiert als TLS-Server und verfügt über ein eindeutiges HAN-Zertifikat CLS_HAN_TLS_CERT. Dieses Zertifikat MUSS vom SMGW genutzt werden, um das CLS zu authentifizieren. [REQ.HAN.HKS4.40]</p> <p>Für das CLS ist im SMGW ein eindeutiger Bezeichner konfiguriert, der auch zur Adressierung des CLS benutzt werden kann.</p>
Aktiver EMT	<p>Der aktive EMT agiert als TLS-Server und verfügt über ein eindeutiges WAN-Zertifikat EMT_WAN_TLS_CERT. Dieses Zertifikat MUSS vom SMGW genutzt werden, um den aktiven EMT zu authentifizieren. [REQ.HAN.HKS4.50]</p> <p>Für den aktiven EMT ist im SMGW ein eindeutiger Bezeichner konfiguriert, welcher zur Adressierung des aktiven EMT benutzt werden kann.</p>

Tabelle 3.17 HKS4: Transparenter Kanal initiiert durch EMT

Umzusetzende Anwendungsfälle

Das SMGW **SOLL** die Kommunikation mit dem CLS für den Anwendungsfall HAF3 über das Kommunikationsszenario HKS4 unterstützen. [REQ.HAN.HKS4.60]



ICS.HAN.HKS4.10

Der GWH **MUSS** im ICS deklarieren, ob das SMGW die Proxy-Kommunikation über HKS4 unterstützt.

3.4.3.5. Kommunikationsszenario HKS5: Transparenter Kommunikationskanal initiiert durch SMGW

Beschreibung

Dieses Szenario beschreibt den Fall, dass das SMGW einen transparenten Kanal zwischen einem CLS und einem aktiven EMT etabliert. Dazu ist es notwendig, dass der GWA die Parameter für die benötigten TLS-Verbindungen zum aktiven EMT und CLS ins SMGW einbringt.

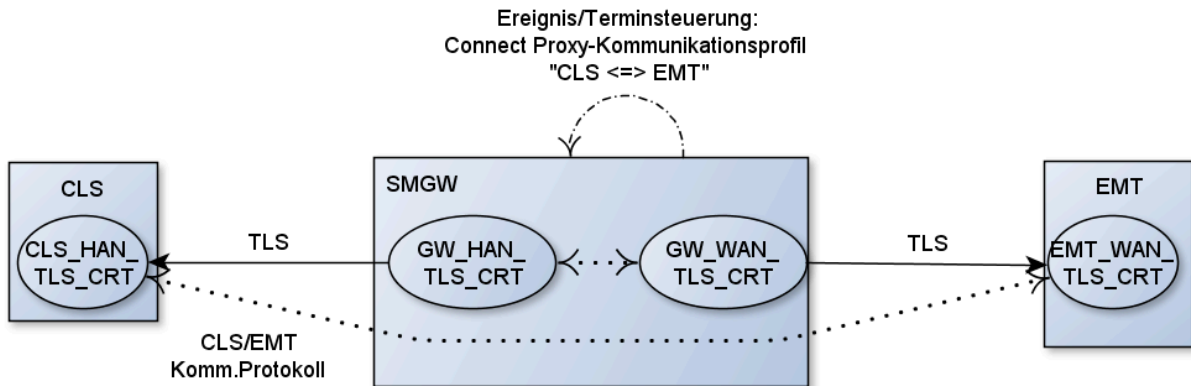


Abbildung 3.18. Transparenter Kanal initiiert durch das SMGW

Im Folgenden werden die notwendigen Prozessschritte genauer betrachtet.

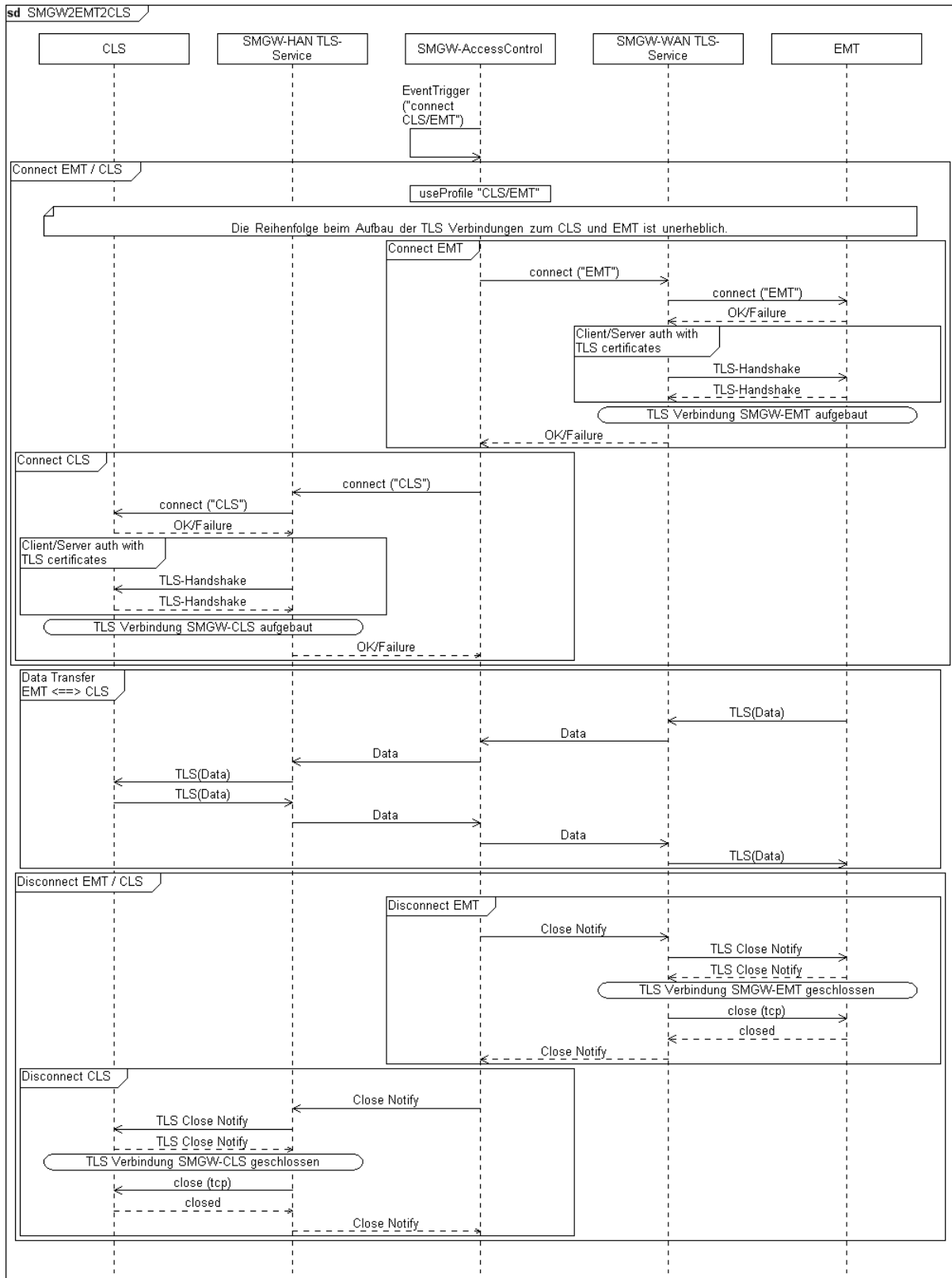


Abbildung 3.19. Sequenzdiagramm Transparenter Kommunikationskanal initiiert durch SMGW

Die Ablaufreihenfolge des Sequenzdiagrammes ist beispielhaft. Es ist sinnvoll zunächst die Verbindung vom SMGW zum CLS aufzubauen und im Erfolgsfall die WAN-Verbindung vom SMGW zum aktiven EMT. Dier

TLS-Verbindungsabbau kann sowohl vom SMGW, vom CLS oder vom aktiven EMT initiiert werden. Das SMGW terminiert dann die jeweils andere zum Proxy-Kommunikationskanal gehörende TLS-Verbindung.

- a. Auf dem SMGW ist im Proxy-Kommunikationsprofil der aktive EMT als zulässiger Kommunikationspartner für dieses CLS eingetragen. Des Weiteren ist im Proxy-Kommunikationsprofil durch den Parameter „Ereignis“ hinterlegt, wann das SMGW den transparenten Kanal initiiert.
- b. Aufbau der WAN-TLS-Verbindung vom SMGW zum aktiven EMT:
 - i. TLS Client-Server Identifikation und Authentifizierung mit Hilfe der Zertifikate von SMGW im WAN und des EMT Zertifikats.
 - ii. Protokollierung des Ergebnisses des WAN-Verbindungsaufbaus im System-Log.
- c. Aufbau der HAN-TLS-Verbindung vom SMGW zum CLS:
 - i. TLS Client-Server Identifikation und Authentifizierung mit Hilfe der Zertifikate des SMGW im HAN und des CLS-Zertifikats.
 - ii. Protokollierung des Ergebnisses des HAN-Verbindungsaufbaus im System-Log.
- d. Transparente Datenkommunikation über die beiden etablierten TLS-Verbindungen.
- e. Beenden der TLS-Verbindung.

Notwendige Vorbedingungen

Akteur	Beschreibung
SMGW	<p>SMGW-WAN: Das SMGW MUSS das WAN Kommunikationsszenario TLS-PROXY (Siehe ▶Abschnitt 3.2.3.6) für die Kommunikation mit dem aktiven EMT verwenden. [REQ.HAN.HKS5.10]</p> <p>SMGW-HAN: Das SMGW MUSS als TLS-Client fungieren, über ein eindeutiges HAN-Zertifikat GW_HAN_TLS_CERT verfügen und das zugehörige Schlüsselmaterial im Sicherheitsmodul speichern. [REQ.HAN.HKS5.20]</p> <p>Dieses Zertifikat wird vom CLS zum Aufbau der TLS-Verbindung genutzt und kann verwendet werden um das SMGW zu authentifizieren.</p> <p>Proxy-Kommunikationsprofil: Die Zulässigkeit der Proxy-Verbindung und die Kommunikationsparameter für den Verbindungsaufbau zum aktiven EMT und CLS sind in einem Proxy-Kommunikationsprofil konfiguriert.</p> <p>Das SMGW MUSS sobald die Bedingung zum Aufbau eines Proxy-Kanals in einem Proxy-Kommunikationsprofil vom Typ HKS5 eingetreten ist, den TLS-Verbindungsaufbau zum CLS und zum aktiven EMT initiieren. [REQ.HAN.HKS5.30]</p>
CLS	<p>Das CLS agiert als TLS-Server und verfügt über ein eindeutiges HAN-Zertifikat CLS_HAN_TLS_CERT.</p> <p>Dieses Zertifikat MUSS vom SMGW genutzt werden, um das CLS zu authentifizieren. [REQ.HAN.HKS5.40]</p> <p>Für das CLS ist im SMGW ein eindeutiger Bezeichner konfiguriert, der auch zur Adressierung des CLS benutzt werden kann.</p>

Akteur	Beschreibung
Aktiver EMT	<p>Der aktive EMT agiert als TLS-Server und verfügt über ein eindeutiges WAN-Zertifikat EMT_WAN_TLS_CERT.</p> <p>Dieses Zertifikat MUSS vom SMGW genutzt werden, um den aktiven EMT zu authentifizieren. [REQ.HAN.HKS5.50]</p> <p>Der aktive EMT ist unter einem eindeutigen Bezeichner registriert, welcher zur Adressierung des aktiven EMT benutzt werden kann.</p>

Tabelle 3.18 HKS5: Transparenter Kommunikationskanal initiiert durch das SMGW

Umzusetzende Anwendungsfälle

Das SMGW **SOLL** die Kommunikation mit dem CLS für den Anwendungsfall HAF3 über das Kommunikationsszenario HKS5 unterstützen. [REQ.HAN.HKS5.60]



ICS.HAN.HKS5.10

Der GWH **MUSS** im ICS deklarieren, ob das SMGW die Proxy-Kommunikation über HKS5 unterstützt.

3.4.4. Sicherung der Kommunikationsverbindungen in das HAN

Das SMGW **MUSS** die Kommunikationsverbindungen des SMGW in das HAN oberhalb der Transportschicht mittels TLS gemäß [TR-03109-3] für die HAN-Kommunikation absichern. [REQ.HAN.SicherungKommunikation.10]

Das SMGW **MUSS** sich immer mit seinem HAN Zertifikat GW_HAN_TLS_CERT authentifizieren. [REQ.HAN.SicherungKommunikation.20]

Die Benutzeridentitäten (Anschlussnutzer, Servicetechniker, CLS und deren Zertifikate bzw. Credentials) **MÜSSEN** auf dem SMGW konfiguriert werden, damit diese vom SMGW als vertrauenswürdig akzeptiert werden. [REQ.HAN.SicherungKommunikation.30]

Das SMGW **MUSS** selbstsignierte Zertifikate oder Zertifikate, die nicht aus der SM-PKI stammen akzeptieren. [REQ.HAN.SicherungKommunikation.40]

Die Zertifikate **MÜSSEN** die kryptographischen Anforderungen aus [TR-03109-3] erfüllen. [REQ.HAN.SicherungKommunikation.50]

3.4.4.1. Sicherung der Kommunikation mit dem Anschlussnutzer / Servicetechniker

Erst nach erfolgreicher Authentifizierung des Anschlussnutzers oder Servicetechnikers erfolgt eine Übermittlung von Daten durch das SMGW. Das SMGW **MUSS** ausschließlich Daten übermitteln, die im SMGW dem authentifizierten Anschlussnutzer bzw. Servicetechniker zugeordnet sind. [REQ.HAN.SicherungKommunikationConSrv.10]

Das SMGW **SOLL** einem Anschlussnutzer bzw. Servicetechniker eine Funktion zum sicheren Ausloggen bereitstellen. [REQ.HAN.SicherungKommunikationConSrv.20] ¹³

Das SMGW **MUSS** sicherstellen, dass zur Identifizierung und Authentifizierung von Servicetechnikern gegenüber dem SMGW ausschließlich HAN-Zertifikate SRV_HAN_TLS_CERT gemäß Detailspezifikation ☞ Zertifikatsprofile am HAN verwendet werden. [REQ.HAN.SicherungKommunikationConSrv.40] Das können selbstsignierte Zertifikate oder durch eine CA ausgestellte Zertifikate sein. Die CA wird vom GWH oder GWA betrieben und ihr Zertifikat muss im SMGW parametrisiert sein.

Das SMGW **KANN** dem Servicetechniker eine Zugriffsberechtigung erteilen, wenn ein kurzlebiges SRV_HAN_TLS_CERT gemäß Detailspezifikation ☞ Zertifikatsprofile am HAN von einer CA ausgestellt wurde,

¹³ Ausloggen bezeichnet das Beenden einer Authentifizierung des Nutzers auf Anwendungs- oder Transportsicherungsebene.

deren *GWACA_SIG_CERT* oder *GWHCA_SIG_CERT* vom GWA im SMGW parametrierung wurde und gültig ist. [REQ.HAN.SicherungKommunikationConSrv.50]

Das SMGW **MUSS** die Identifizierung und Authentifizierung von Anschlussnutzern gegenüber dem SMGW mittels HAN-Zertifikaten *CON_HAN_TLS_CERT* gemäß Detailspezifikation ☞ Zertifikatsprofile am HAN oder mittels Credentials gemäß Detailspezifikation ☞ Authentifizierung mittels Kennung und Passwort durchsetzen. [REQ.HAN.SicherungKommunikationConSrv.60]

Das SMGW **MUSS** die Anzahl der aufeinanderfolgenden, erfolglosen Zugriffsversuche (fehlerhafte Identifizierung oder Authentifizierung am HAN) auf maximal 10 beschränken, indem für einen Zeitraum von mindestens 5 Minuten keine weiteren Zugriffsversuche akzeptiert werden. [REQ.HAN.SicherungKommunikationConSrv.70]

Das SMGW **SOLL** die Übermittlung des Passwort-Hashs als Bestandteil der User-Credentials im HAN-Kommunikationsprofil gemäß Detailspezifikation ☞ Authentifizierung mittels Kennung und Passwort akzeptieren. [REQ.HAN.SicherungKommunikationConSrv.80]

Das SMGW **KANN** die Übermittlung eines Passwortes als Bestandteil der User-Credentials im HAN-Kommunikationsprofil für die HTTP-Digest-Authentifizierung nach Detailspezifikation ☞ Authentifizierung mittels Kennung und Passwort akzeptieren sofern die Anforderungen der [TR-02102-1] an Entropie und Länge eines Passwortes erfüllt sind. [REQ.HAN.SicherungKommunikationConSrv.90] Für Neuimplementierung nicht empfohlen.



ICS.HAN.SicherungKommunikationConSrv.10

Der GWH **MUSS** im ICS deklarieren, ob das SMGW eine Funktion zum Ausloggen für den Anschlussnutzer bereitstellt.



ICS.HAN.SicherungKommunikationConSrv.20

Der GWH **MUSS** im ICS deklarieren, ob das SMGW eine Funktion zum Ausloggen für den Servicetechniker bereitstellt.



ICS.HAN.SicherungKommunikationConSrv.30

Der GWH **MUSS** im ICS deklarieren, ob das SMGW Kenntnis des Anschlussnutzer-Passwortes hat und in einer Anlage zum ICS beschreiben, welche Vorgaben das SMGW an das akzeptierte Anschlussnutzer-Passwort stellt.



ICS.HAN.SicherungKommunikationConSrv.40

Der GWH **MUSS** im ICS deklarieren, ob das SMGW die Authentifizierung des Servicetechnikers mit kurzlebigen Zertifikaten ausgestellt durch eine CA gemäß Detailspezifikation ☞ Zertifikatsprofile am HAN unterstützt.



ICS.HAN.SicherungKommunikationConSrv.50

Der GWH **MUSS** im ICS deklarieren, nach welcher Zahl erfolgloser Zugriffsversuche das SMGW gemäß ▶REQ.HAN.SicherungKommunikationConSrv.60 vorübergehend keine Zugriffsversuche mehr akzeptiert. Sofern die Zahl konfigurierbar ist, ist der Wertebereich zu beschreiben.



ICS.HAN.SicherungKommunikationConSrv.60

Der GWH **MUSS** im ICS deklarieren, für welchen Zeitraum das SMGW gemäß ▶REQ.HAN.SicherungKommunikationConSrv.60 keine weiteren Zugriffsversuche akzeptiert. Sofern die Zahl konfigurierbar ist, ist der Wertebereich zu beschreiben.



ICS.HAN.SicherungKommunikationConSrv.70

Der GWH **MUSS** im ICS deklarieren, ob das SMGW gemäß ▶REQ.HAN.SicherungKommunikationConSrv.50 die Authentifizierung des Servicetechnikers mithilfe eines von einer CA ausgestellten Zertifikats unterstützt.

3.4.4.2. Sicherung der Kommunikation zwischen CLS und aktivem EMT

Das SMGW **MUSS** eine sichere Kommunikation zwischen CLS im HAN und konfigurierten EMT im WAN ermöglichen. Hierzu **MUSS** das SMGW eine Proxy Funktionalität bereitstellen, die eine gesicherte Verbindung des SMGW mit einem CLS auf eine gesicherte Verbindung des SMGW mit einem aktiven EMT abbildet. [REQ.HAN.SicherungKommunikationCls.10] Dies illustriert die folgende Abbildung.

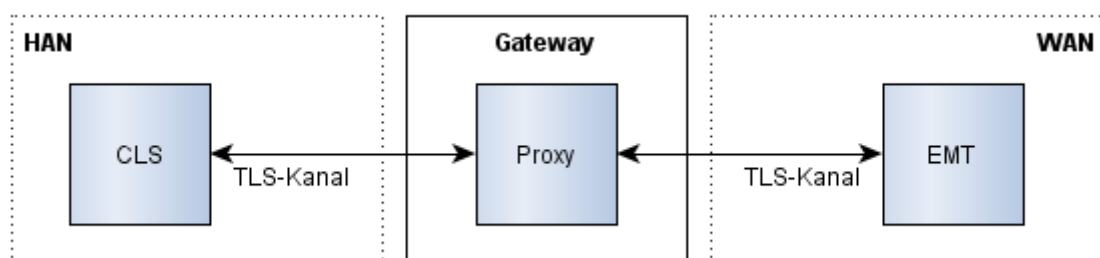


Abbildung 3.20. Absicherung der Kommunikation zwischen CLS und aktivem EMT

Für die Kommunikation zwischen CLS und dem SMGW **MUSS** immer eine beidseitig auf Zertifikaten basierende authentifizierte TLS-Verbindung aufgebaut werden. [REQ.HAN.SicherungKommunikationCls.20]

Das SMGW **MUSS** sicherstellen, dass zur Identifizierung und Authentifizierung von CLS gegenüber dem SMGW ausschließlich HAN-Zertifikate gemäß Detailspezifikation ☞ Zertifikatsprofile am HAN verwendet werden. [REQ.HAN.SicherungKommunikationCls.30]

3.4.5. Kommunikationsprofile im HAN

3.4.5.1. Einleitung

Die Konfiguration der Kommunikation zwischen SMGW und autorisierten Teilnehmern im HAN sowie die Konfiguration für den Aufbau eines transparenten Kommunikationskanals zwischen CLS und autorisierten EMT im WAN wird in HAN- und Proxy-Kommunikationsprofilen festgelegt. Diese werden vom GWA in das SMGW eingespielt.

3.4.5.2. HAN-Kommunikationsprofile

HAN-Kommunikationsprofile legen die Parameter für die Kommunikation des SMGW zu Anschlussnutzern oder Servicetechnikern fest.

Das SMGW **MUSS** in HAN-Kommunikationsprofilen mindestens die folgenden Parameter akzeptieren: [REQ.HAN.Kommunikationsprofile.10]

Parameter	Datentyp / Wertebereich ¹⁴	Beschreibung
Bezeichner	Alphanumerisch	Der im SMGW eindeutige Bezeichner des HAN-Kommunikationsprofils.

¹⁴ Die hier dargestellten Datentypen und Wertebereiche besitzen informativen Charakter.

Parameter	Datentyp / Wertebereich ¹⁴	Beschreibung
Rolle	Einer aus: Anschlussnutzer (CON) Servicetechniker (SRV)	Legt die Rolle des lokalen Nutzers fest.
Kommunikationsszenario	Einer aus: HKS1 HKS2	Legt das Kommunikationsszenario gemäß ▶ Abschnitt 3.4.3 fest.
Wartezeit im Leerlauf	0..n Sekunden	Nach Ablauf der Zeit im Leerlauf, wird die TLS-Verbindung wieder abgebaut. Der Wert 0 deaktiviert den Abbau im Leerlauf.
Maximale Sitzungslänge (optional)	30..172800 Sekunden	Die maximale Zeit, die eine TLS-Sitzung aufgebaut bleiben soll. Ein Wert größer als 48h darf vom SMGW nicht akzeptiert werden. [REQ.HAN.Kommunikationsprofile.20]
Zertifikat des Kommunikationspartners für die TLS-Authentifizierung oder das Signatur-Zertifikat seiner CA (in Abhängigkeit des Kommunikationsszenarios)	Eines aus: CON_HAN_TLS_CERT SRV_HAN_TLS_CERT GWACA_SIG_CERT GWHCA_SIG_CERT	Einer aus: <ul style="list-style-type: none"> Das Zertifikat für die TLS-Authentifizierung des Kommunikationspartners durch das SMGW (Direct-Trust) Das Signatur-Zertifikat einer CA, mit dem ein kurzlebige Zertifikat des Servicetechnikers validiert werden kann.
UserAuth (in Abhängigkeit des Kommunikationsszenarios)	Text	Die zur Überprüfung von Username und Passwort notwendigen Informationen, wie z.B. Information über Credential-Typ, Passwort-Hash und eindeutige Kennung des Anschlussnutzers. Für das HTTP Digest-Authentifizierungsverfahren ist es nicht erforderlich, dass das SMGW Kenntnis des Passwortes selbst hat. Ist im Kommunikationsszenario ein Zertifikat vorgesehen, so bleibt dieses Feld leer.
Zertifikat des SMGW für die TLS-Authentifizierung	GW_HAN_TLS_CERT	Ein Zertifikat des SMGW für die TLS-Authentifizierung durch den Kommunikationspartner.

Tabelle 3.19 Durch HAN-Kommunikationsprofile festzulegende Parameter

Werden optionale Parameter nicht vom GWA übermittelt, so werden die Werte vom SMGW bestimmt.

Das SMGW **KANN** weitere Parameter für HAN-Kommunikationsprofile unterstützen. [REQ.HAN.Kommunikationsprofile.30]

Das SMGW **DARF** dem GWA die Möglichkeit bereitstellen, die Zertifikate des SMGW mithilfe einer vom HAN-Kommunikationsprofil unabhängigen Datenstruktur einzuspielen. [REQ.HAN.Kommunikationsprofile.40] In diesem Fall entfällt die Notwendigkeit diese Parameter als Teil des HAN-Kommunikationsprofils zu akzeptieren.

HAN-Kommunikationsprofile **MÜSSEN** ausschließlich vom GWA eingespielt werden können. [REQ.HAN.Kommunikationsprofile.50]

¹⁴ Die hier dargestellten Datentypen und Wertebereiche besitzen informativen Charakter.

- Vor der Aktivierung des HAN-Kommunikationsprofils **MUSS** das SMGW sicherstellen, dass falls als Rolle der Servicetechniker festgelegt ist, als Kommunikationsszenario HKS1 eingetragen ist. [REQ.HAN.Kommunikationsprofile.70]
- Vor der Aktivierung des HAN-Kommunikationsprofils **MUSS** das SMGW sicherstellen, dass falls als Rolle der Anschlussnutzer festgelegt ist, als Kommunikationsszenario HKS1 oder HKS2 eingetragen ist. [REQ.HAN.Kommunikationsprofile.80]



ICS.HAN.Kommunikationsprofile.10

Der GWH **MUSS** im ICS alle weiteren Parameter für HAN-Kommunikationsprofile beschreiben, die gemäß ▶REQ.HAN.Kommunikationsprofile.30 vom SMGW zusätzlich unterstützt werden.

3.4.5.3. Proxy-Kommunikationsprofile

Die transparente Datenkommunikation zwischen CLS und EMT erfordert die Konfiguration sogenannter *Proxy-Kommunikationsprofile* im SMGW. In einem Proxy-Kommunikationsprofil wird ein CLS mit einem bestimmten EMT verknüpft, indem die notwendigen Kommunikationsparameter der Verbindungsendpunkte spezifiziert werden. Es können mehrere Proxy-Kommunikationsprofile je CLS/EMT definiert werden.

Die Initiierung einer solchen transparenten Datenkommunikation gemäß den Kommunikationsszenarien HKS3 bis HKS5 (s. ▶Abschnitt 3.4.3) kann entweder durch das CLS, den EMT oder durch das SMGW erfolgen.

Proxy-Kommunikationsprofile legen die Parameter für den Aufbau eines transparenten Kommunikationskanals zwischen EMT und CLS fest.

Das SMGW **MUSS** die folgenden Parameter innerhalb von Proxy-Kommunikationsprofilen akzeptieren. [REQ.HAN.ProxyKommunikationsprofile.10]

Parameter	Datentyp / Wertebereich ¹⁵	Beschreibung
Bezeichner	Alphanumerisch	Der im SMGW eindeutige Bezeichner des Proxy-Kommunikationsprofil.
Kommunikationsszenario	Eines aus: HKS3 HKS4 HKS5	Legt das Kommunikationsszenario gemäß ▶Abschnitt 3.4.3 fest.
CLS-ID	Alphanumerisch	Eindeutiger Bezeichner des CLS.
EMT-ID	Alphanumerisch	Eindeutiger Bezeichner des EMT.
Adresse(n) des Kommunikationspartners EMT	Text	Legt eine oder mehrere Adressen fest, über die der Kommunikationspartner erreichbar ist und zu der ein TLS-Kanal aufgebaut werden kann.
Adresse(n) des Kommunikationspartners CLS (optional)	Text	Für HKS4 und HKS5 benötigt.
CLS-Proxy Priorität (optional)	Text	Das Feld CLS-Proxy Priorität bietet die Möglichkeit zu definieren, welches Proxy-Kommunikationsprofil und damit welcher aktive EMT Vorrang bekommt bei Konfliktsituationen zwischen mehreren Proxy-Verbindungen.

¹⁵ Die hier dargestellten Datentypen und Wertebereiche besitzen informativen Charakter.

Parameter	Datentyp / Wertebereich ¹⁵	Beschreibung
Proxy-Start-Ereignis (optional)	Datum, Uhrzeit	Legt das Ereignis fest, bei dem ein Proxy-Kanal zwischen CLS und EMT vom SMGW aufgebaut wird. Dies kann auch ein zeitgesteuerter oder zyklischer Aufbau sein. Nur bei Verwendung des Kommunikationsszenarios HKS5 zu verwenden.
Keepalive (WAN, HAN) (optional)	Boolean / Ja/Nein	Legt fest, ob die TLS-Verbindung dauerhaft aufgebaut bleiben soll, auch wenn die Aktion, die zum Aufbau geführt hat, nicht mehr aktiv ist. Der Kanal wird erst dann geschlossen, wenn die maximale Sitzungslänge erreicht ist. Im anderen Fall wird der Kanal geschlossen, sobald die Aktion beendet ist.
Wiederholung im Fehlerfall (WAN, HAN) (optional)	0..n	Anzahl der TLS-Verbindungsaufbauversuche im Fehlerfall. Führen alle Versuche zu einem Fehler, so muss das Ereignis im System-Log eingetragen werden.
Wartezeit im Fehlerfall (WAN, HAN) (optional)	1..n Sekunden	Die Wartezeit zwischen Verbindungsaufbauversuchen.
Wartezeit im Leerlauf (WAN, HAN) (optional)	0..n Sekunden	Nach Ablauf der Zeit im Leerlauf, wird die TLS-Verbindung wieder abgebaut. Der Wert 0 deaktiviert den Abbau im Leerlauf.
Maximale Sitzungslänge (WAN, HAN) (optional)	30..172800 Sekunden	Die maximale Zeit, die eine TLS-Sitzung bestehen bleiben soll. Ein Wert größer als 48h darf vom SMGW nicht akzeptiert werden.
Zertifikat des aktiven EMT für die TLS-Authentifizierung	EMT_WAN_TLS_CRT	Das Zertifikat für die TLS-Authentifizierung des Kommunikationspartners EMT durch das SMGW.
SubCA-Zertifikat zum TLS-Zertifikat des aktiven EMT	SUBCA_WAN_SIG_CRT	Das Zertifikat der SubCA, welche das TLS-Zertifikat des aktiven EMT innerhalb dieses Profils ausgestellt hat.
Zertifikat des CLS für die TLS-Authentifizierung	CLS_HAN_TLS_CRT	Das Zertifikat für die TLS-Authentifizierung des Kommunikationspartners CLS durch das SMGW.
Zertifikat des SMGW für die TLS-Authentifizierung im WAN	GW_WAN_TLS_CRT	Ein Zertifikat des SMGW für die TLS-Authentifizierung durch den Kommunikationspartner im WAN.
Zertifikat des SMGW für die TLS-Authentifizierung im HAN	GW_HAN_TLS_CRT	Ein Zertifikat des SMGW für die TLS-Authentifizierung durch den Kommunikationspartner im HAN.

Tabelle 3.20 Durch Proxy-Kommunikationsprofile festzulegende Parameter

Proxy-Kommunikationsprofile werden über den eindeutigen Profilbezeichner referenziert.

Werden optionale Parameter nicht vom GWA übermittelt, so werden die Werte vom SMGW bestimmt.

Das SMGW **KANN** weitere Parameter für Proxy-Kommunikationsprofile unterstützen. [REQ.HAN.Proxy-Kommunikationsprofile.20]

¹⁵ Die hier dargestellten Datentypen und Wertebereiche besitzen informativen Charakter.

Das SMGW **DARF** dem GWA die Möglichkeit bereitstellen, die Zertifikate des SMGW mithilfe einer vom HAN-Kommunikationsprofil unabhängigen Datenstruktur einzuspielen. [REQ.HAN.ProxyKommunikationsprofile.30] In diesem Fall entfällt die Notwendigkeit diese Parameter als Teil des Proxy-Kommunikationsprofils zu akzeptieren.

Proxy-Kommunikationsprofile **MÜSSEN** nur vom GWA eingespielt werden können. [REQ.HAN.ProxyKommunikationsprofile.40]



ICS.HAN.ProxyKommunikationsprofile.10

Der GWA **MUSS** im ICS alle weiteren Parameter für Proxy-Kommunikationsprofile beschreiben, die gemäß ▶REQ.HAN.ProxyKommunikationsprofile.20 vom SMGW zusätzlich unterstützt werden.

3.4.6. HAN-Kommunikationsprotokolle

Die Kommunikation des SMGW über das HAN mit dem Anschlussnutzer, Servicetechniker, CLS wird über die in ▶Abbildung 3.21 dargestellten Protokollstapel durchgeführt:

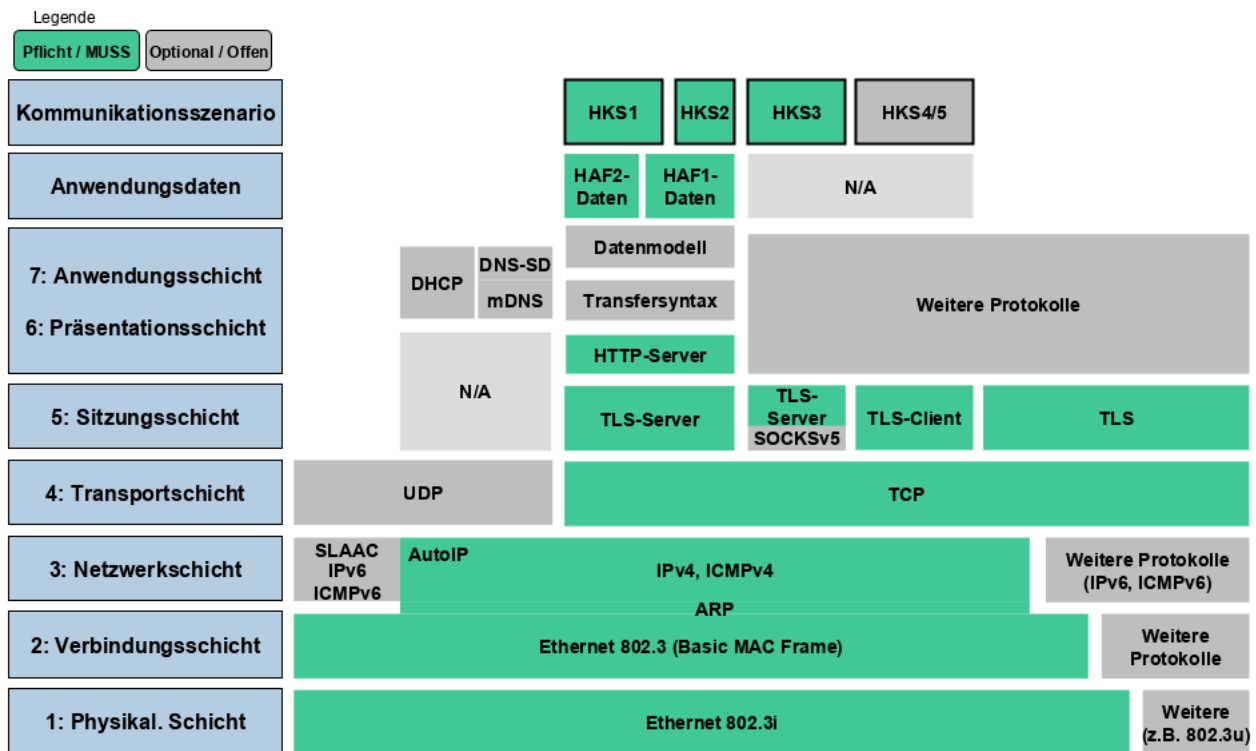


Abbildung 3.21. Protokollstapel für die HAN-Kommunikation

3.4.6.1. Transport von TLS

Um einen zuverlässigen und interoperablen Transport von TLS-Records im HAN zu gewährleisten, **MUSS** das SMGW das TCP/IP Protokoll verwenden. [REQ.HAN.Transport.10]

Das SMGW **MUSS** das TCP/IPv4-Protokoll an der HAN-Schnittstelle für die TLS-Verbindungen verwenden können. [REQ.HAN.Transport.20]

3.4.6.2. Physische HAN-Schnittstellen

Das SMGW **MUSS** eine für den Anschlussnutzer und Servicetechniker in der Einbausituation zugängliche, physische HAN-Schnittstelle besitzen. [REQ.HAN.PhysSchnittstelle.10] Bei der Zugänglichkeit ist zu berücksichtigen, dass der Anschlussnutzer im Regelfall keine Elektrofachkraft ist.

Diese Schnittstelle **MUSS** als Ethernet-Schnittstelle mit einer Geschwindigkeit von mindestens 10 MBit/s (interoperabel mit [IEEE 802.3i]) ausgelegt sein. [REQ.HAN.PhysSchnittstelle.20]

Das SMGW **MUSS** IPv4 an der HAN-Schnittstelle unterstützen. [REQ.HAN.PhysSchnittstelle.30]

Das SMGW **SOLL** IPv6 an der HAN-Schnittstelle unterstützen. [REQ.HAN.PhysSchnittstelle.40]

Das SMGW **SOLL** die automatische Adresskonfiguration an der HAN-Schnittstelle nach Detailspezifikation ☞ Detailspezifikation Automatische Adresskonfiguration und DNS-Discovery unterstützen, so dass ein HAN-Teilnehmer in der Lage ist, ohne vorherige Netzwerkkonfiguration Dienste des SMGW in Anspruch nehmen zu können. [REQ.HAN.PhysSchnittstelle.50]

Die Absicherung der Kommunikation **MUSS** über TLS gemäß den Anforderungen aus [TR-03109-3] erfolgen. [REQ.HAN.PhysSchnittstelle.60]

Weitere HAN-Schnittstellen, die den obigen Anforderungen genügen, **KÖNNEN** am SMGW bereitgestellt werden. [REQ.HAN.PhysSchnittstelle.70]



ICS.HAN.PhysSchnittstelle.10

Der GWH **MUSS** im ICS deklarieren, ob das SMGW IPv6 an der HAN-Schnittstelle unterstützt.



ICS.HAN.PhysSchnittstelle.20

Der GWH **MUSS** im ICS deklarieren, wie viele physische HAN-Schnittstellen das SMGW besitzt.



ICS.HAN.PhysSchnittstelle.30

Der GWH **MUSS** im ICS deklarieren, ob das SMGW die automatische Adresskonfiguration nach Detailspezifikation ☞ Detailspezifikation Automatische Adresskonfiguration und DNS-Discovery unterstützt.

4. Messwertverarbeitung für Tarifierung, Bilanzierung und Netzzustandsdatenerhebung

4.1. Einleitung

In diesem Kapitel wird die dezentrale Messwertverarbeitung für bestimmte Anwendungszwecke wie der *Tarifierung* von Verbrauchs- und Einspeisemengen sowie für die Erhebung von Netzzustandsdaten für das SMGW beschrieben. Dabei muss das SMGW auch Messdaten erheben können, die von Netzbetreibern u.a. für die Bilanzierung von Energienetzen verwendet werden. Regelwerke im SMGW bestimmen, wie Messwerte für Auswertungen verwendet werden.

In diesem Kapitel werden Mindestanforderungen an die Messwertverarbeitung gestellt.

- ▶Abschnitt 4.2 geht auf die Anwendungsfälle ein, die als Minimum vom SMGW unterstützt werden müssen.
- ▶Abschnitt 4.3 stellt das Konzept der Messwertverarbeitung im SMGW vor.
- ▶Abschnitt 4.4 beschreibt die Konfigurationsprofile für die Messwertverarbeitung.
- ▶Abschnitt 4.5 stellt Anforderungen an Zugriffsberechtigungen.

4.2. Anwendungsfälle für Regelwerke

4.2.1. Einleitung

▶Abschnitt 4.2 enthält Anwendungsfälle für Tarifierung, Bilanzierung und Netzzustandsdatenerhebung, die vom SMGW durch Regelwerke umgesetzt werden **MÜSSEN**. Diese sind in ▶Tabelle 4.1 aufgelistet. [REQ.M-WV.TafAllgemein.10] Die Anforderungen sind dabei, losgelöst von einer technischen Ausgestaltung der Regelwerke, auf übergeordneter Ebene beschrieben.

Jeder Anwendungsfall (gekennzeichnet mit dem Kürzel TAF) wird tabellarisch jeweils unter Angabe der folgenden Informationen beschrieben:

- Allgemeine Beschreibung des Anwendungsfalls.
- Relevante Parameter für die Parametrierung des Anwendungsfalls.
- Die im Anwendungsfall dem EMT bereitzustellenden Daten.
- Die vom SMGW für den Anschlussnutzer an der HAN-Schnittstelle als Minimum bereitzustellenden Daten.

Die nachfolgende ▶Tabelle 4.1 listet alle in ▶Abschnitt 4.2 beschriebenen Anwendungsfälle auf.

Abschnitt	Anwendungsfall	Abrechnungsrelevant
▶4.2.2	TAF1: Datensparsame Tarife	ja
▶4.2.3	TAF2: Zeitvariable Tarife	ja
▶4.2.4	TAF6: Ablesung von Messwerten im Bedarfsfall	ja
▶4.2.5	TAF7: Zählerstandsgangmessung	ja
▶4.2.6	TAF9: Abruf der Ist-Einspeisung	nein

Abschnitt	Anwendungsfall	Abrechnungsrelevant
►4.2.7	TAF10: Abruf von Netzzustandsdaten	nein
►4.2.8	TAF14: Hochfrequente Messwertbereitstellung für Mehrwertdienste	nein

Tabelle 4.1 Zuordnung der Anwendungsfälle zu den jeweiligen Auslösern im Regelwerk

4.2.2. TAF1: Datensparsame Tarife

4.2.2.1. Beschreibung

Dieser Anwendungsfall beschreibt Tarife, die für Verbrauchsabrechnungen herangezogen werden können, bei denen ein hohes Interesse an Datensparsamkeit besteht. Diese Datensparsamkeit soll verhindern, dass auf Basis der vom SMGW versandten Messwerte, Auswertungen über das Verbrauchsverhalten des Anschlussnutzers getätigt werden können. Der Anwendungsfall betrachtet nur eine Tarifstufe.

Zu diesem Zweck **MUSS** das SMGW von einem angeschlossenen Zähler genau einen (1) *Zählerstand* pro erfasster Messgröße und *Abrechnungszeitraum* an autorisierte EMT versenden. [REQ.MWV.Taf1.10] Das SMGW **MUSS** Abrechnungszeiträume von einem (1) Monat und ein Vielfaches hiervon ermöglichen. [REQ.MWV.Taf1.20] Das **SMGW MUSS** die Zählerstände in der zugeordneten Messwertliste eintragen. [REQ.MWV.Taf1.30]

Zeitstempel	Grund ¹	Zählerstand in kWh
01.02.2013 0:00:00h	Monatliche Ablesung	512
01.03.2013 0:00:00h	Monatliche Ablesung	545
01.04.2013 0:00:00h	Monatliche Ablesung	567
01.05.2013 0:00:00h	Monatliche Ablesung	577
...

Tabelle 4.2 Beispiel für einen einfachen Tarif mit minimalem Datenversand bei monatlicher Abrechnung

Zähler und Messgrößen werden über die *Geräte-IDs* der Zähler und die OBIS-Kennzahlen der zu erfassenden Messgrößen ausgewählt.

Das SMGW **MUSS** zu den definierten Versandzeitpunkten die erfassten Zählerstände an die berechtigten EMT versenden. [REQ.MWV.Taf1.40] Über die parametrisierten Berechtigungen wird geregelt, welcher EMT berechtigt ist.

Das SMGW **MUSS** die in diesem Anwendungsfall zu versendenden Daten vor der Inhaltsdatenverschlüsselung mit einer zusätzlichen Signatur versehen. [REQ.MWV.Taf1.50]

Das SMGW stellt dem Anschlussnutzer zu diesem Anwendungsfall Daten über die HAN-Schnittstelle bereit (s. ►Abschnitt 4.2.2.4). Über eine Anschlussnutzerkennung ist der Tarif mit dem Anschlussnutzer verknüpft.

Das SMGW **MUSS** den Betrieb des Regelwerks zu Beginn des *Gültigkeitszeitraums* oder, falls der Beginn des Gültigkeitszeitraums in der Vergangenheit liegt, zum Zeitpunkt des Einspielens (sofern gemäß ►ICS.MWV.Taf1Parameter.10 unterstützt) aufnehmen. [REQ.MWV.Taf1.60] Das SMGW **MUSS** den Betrieb des Regelwerks zum Ende des Gültigkeitszeitraums einstellen. [REQ.MWV.Taf1.70] Eine rückwirkende Tarifierung ist bei einem neu eingespielten Auswertungsprofil mit einem in der Vergangenheit liegenden Startzeitpunkt für den Gültigkeitszeitraum auszuschließen. Auch bei einer sofortigen Aufnahme des Betriebs des Regelwerks ist das Raster, das durch die Registrierperiode vorgegeben wird, einzuhalten (siehe *Sollregistrierzeitpunkt*).

4.2.2.2. Notwendige Parameter für das Regelwerk

Das SMGW **MUSS** die folgenden Parameter zur Parametrierung eines TAF1 akzeptieren: [REQ.MWV.Taf1Parameter.10]

¹ Die gezeigten Ereignistexte sollen nur die Art des Ereignisses darstellen und nicht festlegen, wie diese zu kodieren sind.

Parameter	Beschreibung
Geräte-ID des Zählers	Der eindeutige Bezeichner des Zählers.
OBIS-Kennzahl der zu verwendenden Messgröße je Zähler	Die eindeutige Kennzahl der für den Tarif zu verwendenden Messgrößen des jeweiligen Zählers.
Zählpunktbezeichnung	Der eindeutige Bezeichner der <i>Messlokation</i> .
Registrierperiode	Der zeitliche Abstand zwischen zwei aufeinanderfolgenden Messwerterfassungen.
Abrechnungszeitraum	Der Zeitraum für den Messwerte für die Abrechnung ermittelt werden müssen.
Anschlussnutzerkennung	Die eindeutige Kennung des Anschlussnutzers, der die angefallenen Daten einsehen darf.
Berechtigungen	Berechtigungen, die regeln, wer die ermittelten Daten über HAN oder WAN erhalten oder auslesen darf.
Versandzeitpunkte	Die Zeitpunkte zu denen die ermittelten Daten vom SMGW versendet werden.
Gültigkeitszeitraum	Der Zeitraum für den das Regelwerk im SMGW verwendet werden soll.

Tabelle 4.3 Regelwerkparameter für TAF1



ICS.MWV.Taf1Parameter.10

Der GWH **MUSS** im ICS angeben, ob das SMGW einen Zeitpunkt in der Vergangenheit für den Beginn des Gültigkeitszeitraums gemäß ▶REQ.MWV.Taf1.60 akzeptiert und den Betrieb des Regelwerks in diesem Fall zum Einspielzeitpunkt aufnimmt.

4.2.2.3. Vom Regelwerk für EMT bereitzustellende Daten

- Das SMGW **MUSS** dem EMT für diesen TAF1 den Zählerstand pro erfasster Messgröße am Ende des jeweiligen Abrechnungszeitraums bereitstellen. [REQ.MWV.Taf1EmtDaten.10]
- Das SMGW **MUSS** dem EMT für diesen TAF1 den Bezeichner des zugehörigen Auswertungsprofils bereitstellen. [REQ.MWV.Taf1EmtDaten.20]

4.2.2.4. Für den jeweiligen Anschlussnutzer an der HAN-Schnittstelle bereitzustellende Daten

- Das SMGW **MUSS** dem Anschlussnutzer an der HAN-Schnittstelle den Zählerstand pro erfasster Messgröße zum Ende des letzten Abrechnungszeitraums bereitstellen. [REQ.MWV.Taf1AnDaten.10]
- Das SMGW **MUSS** dem Anschlussnutzer an der HAN-Schnittstelle die Messwertliste bereitstellen. [REQ.MWV.Taf1AnDaten.20]
- Weitere Daten gemäß den Anforderungen in ▶Abschnitt 3.4.2.1.

4.2.3. TAF2: Zeitvariable Tarife

Für ▶Abschnitt 4.2.3 werden folgende sprachlichen Vereinbarungen getroffen:

Ein Messwert geht *rechtzeitig* zu einem *Sollregistrierzeitpunkt* im SMGW ein, wenn die technischen Anforderungen nach [MessEG]/[MessEV] an den Empfangszeitpunkt im SMGW erfüllt sind.

Ein Messwert wird als *fehlerfrei* bezeichnet, wenn der Zähler keinen Fehler zu dem Messwert mitsendet, die Integrität und Authentizität des Messwertes erfolgreich vom SMGW geprüft wurden und das SMGW selbst keinen abrechnungsrelevanten Fehler besitzt.

Ein Messwert ist *valide*, wenn er fehlerfrei ist und rechtzeitig im SMGW eingeht.

4.2.3.1. Beschreibung

Dieser Anwendungsfall ermöglicht es Energiemengen in Abhängigkeit der Zeit in unterschiedlichen *Registern* zu erfassen. Hiermit können zeitvariable Tarife realisiert werden, bei denen der Lieferant dem Anschlussnutzer zeitabhängig für die bezogene Energie unterschiedliche Preise in Rechnung stellt.



Anmerkung

Der Anwendungsfall ermöglicht neben der Erfassung von zeitlich variablen Verbräuchen analog auch die Erfassung von zeitlich variablen *Einspeisungen*. In diesem Fall liefert der Zähler Messwerte für die eingespeiste Energie anstelle der bezogenen Energie. Zur besseren Lesbarkeit beschränken sich die folgenden Absätze auf den Bezugsfall; die Aussagen gelten jedoch analog für den Einspeisefall.

Die Konfiguration der Register sowie der Umschaltzeitpunkte zwischen diesen erfolgt über Auswertungsprofile, an die jeweils *Zeitbedingungen* geknüpft sind. Die Zeitbedingungen definieren *Tarifumschaltzeitpunkte*. Ein aktives Register bleibt jeweils bis zum nächsten Tarifumschaltzeitpunkt aktiv. Die Zeitbedingungen müssen so gewählt sein, dass zu jedem Zeitpunkt des Gültigkeitszeitraums genau ein Register pro Auswertungsprofil aktiv ist. Das SMGW **MUSS** die anfallenden Energiemengen in dem jeweils aktiven abgeleiteten Register kumulieren. [REQ.MWV.Taf2.10] Auf diese Weise wird die gesamte, innerhalb des Abrechnungszeitraumes angefallene Energiemenge auf die Register verteilt. Das SMGW **MUSS** ein Fehlerregister für nicht eindeutig zuordenbare Energiemengen vorhalten (nachfolgend als "Register 63" bezeichnet). [REQ.MWV.Taf2.20] Das SMGW **MUSS** ein Gesamtregister für die gesamte verbrauchte Energiemenge vorhalten (nachfolgend als "Register 0" bezeichnet). [REQ.MWV.Taf2.30]

Es wird im Folgenden davon ausgegangen, dass pro Auswertungsprofil nur ein (1) Zähler konfiguriert wurde. Die zeitvariable Verarbeitung von Daten mehrerer Zähler (Verrechnung in einem Auswertungsprofil) ist nicht Bestandteil dieser Beschreibung und soll damit nicht umgesetzt werden.

Jedes Register erhält eine eindeutige OBIS-Kennzahl gemäß der Parametrierung im Auswertungsprofil.

Zu Beginn des Gültigkeitszeitraums (s. ▶Tabelle 4.5) **MUSS** das SMGW den Wert 0 in jedes abgeleitete Register eintragen. [REQ.MWV.Taf2.40] Bei Eintritt eines Sollregistrierzeitpunktes **MUSS** das SMGW den Zählerstand von einem Zähler erfassen, einen Eintrag in der Liste der originären Messwerte erzeugen und die am Zähler zwischen den letzten beiden Sollregistrierzeitpunkten angefallene Energiemenge zu dem währenddessen aktiven Register kumulieren (Beispiel für Entwicklung bei HT/NT-Tarifen s. ▶Abbildung 4.1). [REQ.MWV.Taf2.50] Die genaue Vorgehensweise wird in ▶Abschnitt 4.2.3.2 bis ▶Abschnitt 4.2.3.5 erläutert. Das SMGW hat der Beschreibung zu folgen und **DARF** die Register während des gesamten Gültigkeitszeitraums **NICHT** auf den Wert 0 zurücksetzen. [REQ.MWV.Taf2.60] Eine rückwirkende Tarifierung ist bei einem neu eingespielten Auswertungsprofil mit einem in der Vergangenheit liegenden Startzeitpunkt für den Gültigkeitszeitraum auszuschließen. Auch bei einer sofortigen Aufnahme des Betriebs des Regelwerks ist das Raster, das durch die Registrierperiode vorgegeben wird, einzuhalten (siehe *Sollregistrierzeitpunkt*).

Zähler und Messgrößen der Messwerte werden über die Geräte-ID des Zählers und die OBIS-Kennzahlen der Messgrößen ausgewählt. Das SMGW **MUSS** für diesen Anwendungsfall die in ▶Tabelle 4.4 aufgeführten Größen für eingehende Messwerte unterstützen. [REQ.MWV.Taf2.70]

Das SMGW **MUSS** zu definierten Versandzeitpunkten die Registerwerte an berechnete EMT versenden. [REQ.MWV.Taf2.80] Das SMGW **KANN** zusätzlich die *Tarifwechselliste* an berechnete EMT versenden. [REQ.MWV.Taf2.90] Über die parametrisierten Berechtigungen wird geregelt, welcher EMT berechnete ist.

Das SMGW stellt dem Anschlussnutzer zu diesem Anwendungsfall Daten über die HAN-Schnittstelle bereit (s. ▶Abschnitt 4.2.3.9). Das SMGW **MUSS** darüber hinaus über einen Eintrag im Anschlussnutzer-Log informieren, wenn ein Tarifwechsel stattgefunden hat und welche Tarifstufe jetzt beginnt. [REQ.MWV.Taf2.100] Der jeweilige Anschlussnutzer wird über die Anschlussnutzerkennung identifiziert, die über das Auswertungsprofil dem Zähler zugeordnet sein muss.

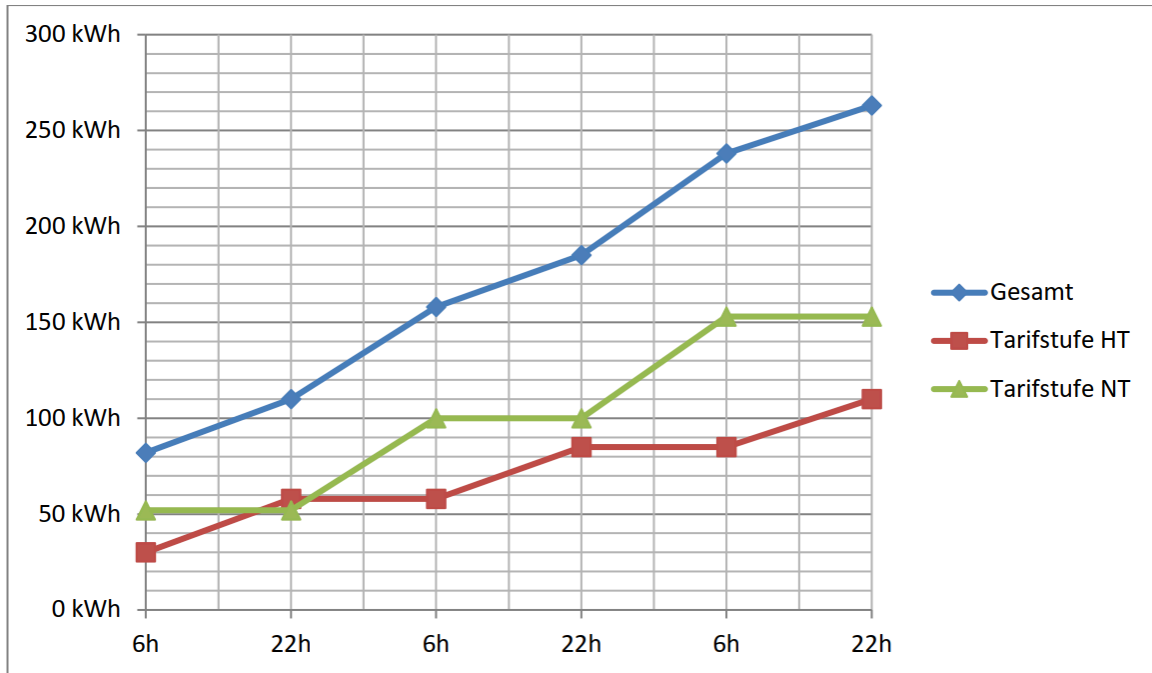


Abbildung 4.1. Beispiel für einen zeitvariablen Tarif mit zwei Tarifstufen (HT/NT)



ICS.MWV.Taf2EmtDaten.10

Der GWH **MUSS** im ICS angeben, ob das SMGW die Tarifwechselliste gemäß ▶REQ.MWV.Taf2.90 und ▶REQ.MWV.Taf2EmtDaten.40 an berechnete EMT versenden kann.

4.2.3.2. Kumulation im fehlerlosen Fall

Das SMGW **MUSS** zum Sollregistrierzeitpunkt t_n den Messwert Z_n mit dem Zeitstempel s_n in die Liste der originären Werte aufnehmen. [REQ.MWV.Taf2Kumulation.10] Sei Register X das aktive Register der abgelaufenen Sollregistrierperiode $[t_{n-1}, t_n]$. Seien Z_{n-1} und Z_n valide Zählerstände in der Messwertliste des SMGW. Dann **MUSS** das SMGW den Registerstand in den Registern 0 und X um die Differenz $Z_n - Z_{n-1}$ erhöhen. [REQ.MWV.Taf2Kumulation.20]

4.2.3.3. Kumulation bei Empfangsstörung

Sei t_m der Sollregistrierzeitpunkt, zu dem zuletzt ein valider Messwert Z_m vom Zähler empfangen/abgerufen werden konnte, und $t_n > t_m$ ein Sollregistrierzeitpunkt, zu dem kein Messwert im Gateway empfangen wurde. Dann **MUSS** das SMGW den Messwert Z_{n-1} des vorherigen Sollregistrierzeitpunkts in der Liste der originären Werte an der Stelle des Sollregistrierzeitpunkts t_n wiederholen und den Messwertstatus entsprechend setzen. [REQ.MWV.Taf2Kumulation.30]

Der *Energievorschub* zwischen t_n und t_{n-1} ist 0, sodass sich die Registerstände zu diesem Zeitpunkt noch nicht ändern.

Wenn nun zu einem späteren Sollregistrierzeitpunkt $t_o > t_n$ wieder ein valider Messwert Z_o empfangen/abgerufen werden kann und alle Messwerte im Zeitraum $[t_m, t_o]$ fehlerfrei sind, müssen zwei Fälle unterschieden werden (s. auch ▶Abbildung 4.2):

Fall 1: Im Zeitraum (t_m, t_o) liegt kein Tarifumschaltzeitpunkt, bei dem sich die Tarifstufe geändert hat. Dann **MUSS** das SMGW den Registerstand im Register 0 und dem aktiven Register X um die Differenz $Z_o - Z_m$ erhöhen. [REQ.MWV.Taf2Kumulation.40]

Fall 2: Im Zeitraum (t_m, t_o) liegt mindestens ein Tarifumschaltzeitpunkt, bei dem die Tarifstufe geändert wurde. Der Energievorschub $Z_o - Z_m$ ist damit keinem Register eindeutig zuordenbar. Das SMGW **MUSS** die Differenz $Z_o - Z_m$ zu den Energiemengen in den Registern 0 und 63 addieren. [REQ.MWV.Taf2Kumulation.50]

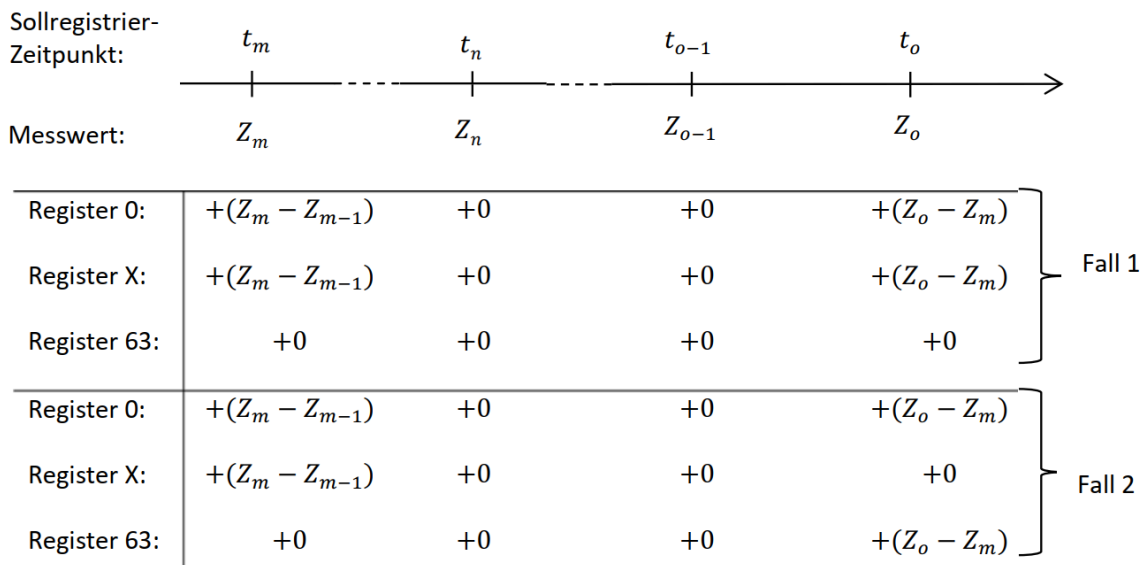


Abbildung 4.2. Kumulation nach Behebung einer Empfangsstörung

Liegt im Zeitraum $[t_m, t_o]$ hingegen ein nicht fehlerfreier Messwert zum Sollregistrierzeitpunkt t_f , dann **MUSS** das SMGW die Differenz $Z_o - Z_f$ zu den Energiemengen in den Registern 0 und 63 addieren. [REQ.MWV.Taf2Kumulation.55]

4.2.3.4. Kumulation bei Überschreitung der zeitlichen Fehlergrenzen

Für die Fälle, in denen die technischen Anforderungen nach [MessEG]/[MessEV] an die Systemzeit des SMGW oder an den Empfangszeitpunkt eines Messwerts nicht erfüllt werden und der Zähler keinen Fehler meldet **MUSS** das SMGW analog zum in ▶Abschnitt 4.2.3.3 geschilderten Fall der Empfangsstörung verfahren. [REQ.MWV.Taf2Kumulation.60] Falls das SMGW gemäß ▶ICS.MWV.Taf2Kumulation.10 Messwerte in diesen Fällen erfasst, **MUSS** das SMGW abweichend zu ▶Abschnitt 4.2.3.3 den nicht validen Messwert Z_n zusammen mit dem Zeitstempel s_n und dem entsprechenden Messwertstatus in der Liste der originären Werte für den Sollregistrierzeitpunkt t_n erfassen. [REQ.MWV.Taf2Kumulation.70]



ICS.MWV.Taf2Kumulation.10

Der GWH **MUSS** im ICS angeben, ob das SMGW Messwerte im Fehlerfall nach ▶REQ.MWV.Taf2Kumulation.70 in der Liste der originären Werte erfasst statt sie zu verwerfen.

4.2.3.5. Kumulation bei Zählerfehlern

Sei t_n der Sollregistrierzeitpunkt des rechtzeitig empfangenen Messwerts Z_n , zu dem der Zähler jedoch einen nicht-fatalen Fehler (d.h. Klemmdeckel offen, magnetische Beeinflussung o.ä.) im Messwertstatus sendet. Sei weiterhin t_m mit $t_m < t_n$ der letzte Sollregistrierzeitpunkt, zu dem der Messwert Z_m entweder mit nicht-fatalem Fehler oder valide erfasst wurde. Messwerte, die nicht rechtzeitig eingegangen aber ansonsten fehlerfrei sind, werden bei der Betrachtung analog zu ▶Abschnitt 4.2.3.3 ignoriert.

Dann ist der Energievorschub von $t_n - t_m$ nicht vollständig vertrauenswürdig und das SMGW **MUSS** dem Fehlerregister 63 sowie dem Register 0 die Differenz $Z_n - Z_m$ hinzufügen. [REQ.MWV.Taf2Kumulation.80] Der Messwert Z_n mit dem Zeitstempel s_n und dem entsprechenden Messwertstatus wird in der Liste der originären Werte für den Sollregistrierzeitpunkt t_n erfasst.

Sei nun nach obigem Szenario erneut Z_o ein valider Messwert, der rechtzeitig zum Sollregistrierzeitpunkt $t_o > t_n$ im SMGW eingeht. Dann **MUSS** das SMGW den Energievorschub $Z_o - Z_n$ dem Fehlerregister 63 sowie dem Register 0 hinzufügen. [REQ.MWV.Taf2Kumulation.90] Nicht rechtzeitig eingegangene Messwerte, die aber ansonsten fehlerfrei sind, werden wie zuvor ignoriert. Wenn im Anschluss wieder valide Messwerte eintreffen, kann wie in ▶Abschnitt 4.2.3.2 beschrieben tarifiert werden.

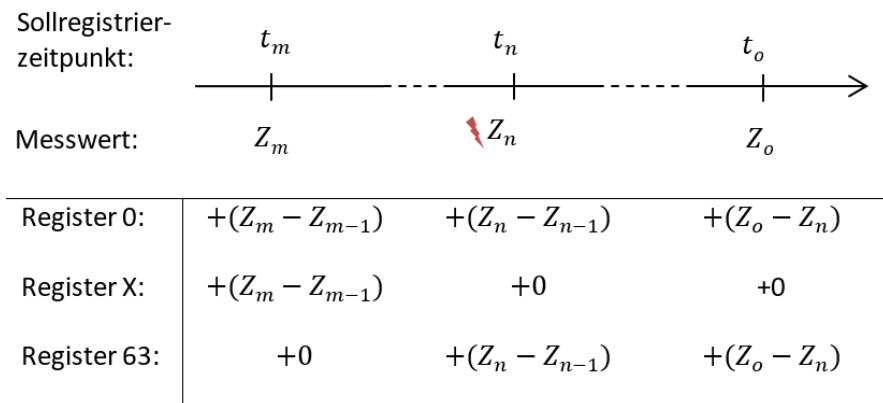


Abbildung 4.3. Kumulation bei fehlerhaften Messwerten

Wenn ein Messwert eingeht, zu dem der Zähler einen fatalen Fehler im Messwertstatus sendet, dann darf das SMGW den Energievorschub keinem der Register mit Ausnahme des Gesamt- und des Fehlerregisters zuordnen. Dies gilt ebenfalls für alle zukünftig von diesem Zähler empfangenen Messwerte. Siehe dazu ▶Abschnitt 4.3.4. Der Zähler muss in diesem Fall ausgetauscht werden.

4.2.3.6. OBIS-Kennzahlen

OBIS-Kennzahl	Messgröße	Messart	Einheit
Elektrizität			
1-0:1.8.0 ²	Wirkarbeit Bezug	Zählerstand	Kilowattstunde (kWh)
1-0:2.8.0	Wirkarbeit Lieferung	Zählerstand	Kilowattstunde (kWh)
1-0:3.8.0	Blindarbeit Bezug	Zählerstand	Kilovoltamperereaktivstunde (kvarh)
1-0:4.8.0	Blindarbeit Lieferung	Zählerstand	Kilovoltamperereaktivstunde (kvarh)
1-0:5.8.0	Blindarbeit Q I	Zählerstand	Kilovoltamperereaktivstunde (kvarh)
1-0:6.8.0	Blindarbeit Q II	Zählerstand	Kilovoltamperereaktivstunde (kvarh)
1-0:7.8.0	Blindarbeit Q III	Zählerstand	Kilovoltamperereaktivstunde (kvarh)
1-0:8.8.0	Blindarbeit Q IV	Zählerstand	Kilovoltamperereaktivstunde (kvarh)

Tabelle 4.4 OBIS-Kennzahlen für abrechnungsfähige originäre Werte

² Hinweis: Gemeint ist der durch den Zähler gelieferte Wert und nicht der Stand des im SMGW vorgehaltenen Registers für die Gesamtenergiemenge.

4.2.3.7. Notwendige Parameter für das Regelwerk

Das SMGW **MUSS** die folgenden Parameter zur Parametrierung eines TAF2 akzeptieren: [REQ.MWV.Taf2Parameter.10]

Parameter	Beschreibung
Geräte-ID des Zählers	Der eindeutige Bezeichner des Zählers.
OBIS-Kennzahl der zu verwendenden Messgröße je Zähler	Die eindeutige Kennzahl der für den Tarif zu verwendenden Messgröße des jeweiligen Zählers.
Zählpunktbezeichnung	Der eindeutige Bezeichner der Messlokation.
Registrierperiode	Der zeitliche Abstand zwischen zwei aufeinanderfolgenden Messwernerfassungen.
Definition der Register	Definiert die verschiedenen Register und die zugehörigen OBIS-Kennzahlen.
Zeitbedingungen	Definieren die Tarifumschaltzeitpunkte und welches Register zum Zeitpunkt der Aktivierung des Regelwerks aktiv ist. Daraus müssen sich die Tarifumschaltzeitpunkte und das zwischen zwei Umschaltzeitpunkten aktive Register ergeben.
Abrechnungszeitraum	Der Zeitraum für den Messwerte für die Abrechnung ermittelt werden müssen.
Anschlussnutzerkennung	Die eindeutige Kennung des Anschlussnutzers, der die angefallenen Daten einsehen darf.
Berechtigungen	Berechtigungen, die regeln, wer die ermittelten Daten über HAN oder WAN erhalten oder auslesen darf.
Versandzeitpunkte	Die Zeitpunkte zu denen die ermittelten Daten an den berechtigten EMT vom SMGW versendet werden
Gültigkeitszeitraum	Der Zeitraum für den das Regelwerk im SMGW verwendet werden soll.

Tabelle 4.5 Regelwerkparameter für TAF2



ICS.MWV.Taf2Parameter.10

Der GWH **MUSS** im ICS angeben, ob das SMGW einen Zeitpunkt in der Vergangenheit für den Beginn des Gültigkeitszeitraums akzeptiert und den Betrieb des Regelwerks in diesem Fall zum Einspielzeitpunkt aufnimmt.

4.2.3.8. Vom Regelwerk für EMT bereitzustellende Daten

- Das SMGW **MUSS** dem EMT für diesen TAF2 den Stand der Register inkl. OBIS-Kennzahlen zum letzten Sollregistrierzeitpunkt des jeweiligen Abrechnungszeitraums inklusive Zeitstempel bereitstellen. [REQ.MWV.Taf2EmitDaten.10]
- Das SMGW **MUSS** dem EMT für diesen TAF2 den Bezeichner des zugehörigen Auswertungsprofils bereitstellen. [REQ.MWV.Taf2EmitDaten.20]
- Das SMGW **MUSS** dem EMT für diesen TAF2 die Geräte-ID des Zählers inkl. Liste der zu verwendenden OBIS-Kennzahlen bereitstellen. [REQ.MWV.Taf2EmitDaten.30]
- Das SMGW **DARF** dem EMT für diesen TAF2 die Liste der Tarifumschaltzeitpunkte bereitstellen. [REQ.MWV.Taf2EmitDaten.40]³

4.2.3.9. Für den jeweiligen Anschlussnutzer an der HAN-Schnittstelle bereitzustellende Daten

- Das SMGW **MUSS** dem Anschlussnutzer an der HAN-Schnittstelle für diesen TAF2 den Stand der Register zum - vom Zeitpunkt des Abrufs aus betrachtet - letzten Sollregistrierzeitpunkt mit Zeitstempel und Status

³ Siehe ▶ ICS.MWV.Taf2EmitDaten.10.

(Unterscheidung valide/nicht-valide ist ausreichend) des Messwertes des letzten Sollregistrierzeitpunkts bereitstellen. [REQ.MWV.Taf2AnDaten.10]

- Das SMGW **MUSS** dem Anschlussnutzer an der HAN-Schnittstelle für diesen TAF2 die Messwertliste inklusive Zeitstempel, zugehörigem Sollregistrierzeitpunkt und Messwertstatus bereitstellen. [REQ.MWV.Taf2AnDaten.20]
- Das SMGW **MUSS** dem Anschlussnutzer an der HAN-Schnittstelle für diesen TAF2 die Liste der Tarifumschaltzeitpunkte bereitstellen. [REQ.MWV.Taf2AnDaten.30]
- Das SMGW **DARF** dem Anschlussnutzer an der HAN-Schnittstelle für diesen TAF2 das aktuell aktive Register bereitstellen. [REQ.MWV.Taf2AnDaten.40]
- Weitere Daten gemäß den Anforderungen in ▶Abschnitt 3.4.2.1.



ICS.MWV.Taf2AnDaten.10

Der GWH **MUSS** im ICS angeben, ob das SMGW dem Anschlussnutzer an der HAN-Schnittstelle das aktuell aktive Register gemäß ▶REQ.MWV.Taf2AnDaten.40 bereitstellt.

4.2.4. TAF6: Abruf von Messwerten im Bedarfsfall

4.2.4.1. Beschreibung

Dieser Anwendungsfall erlaubt den Abruf von Messwerten in nicht planbaren Situationen.

Um rückwirkend Ablesungen zu einem konkreten Stichtag zu ermöglichen, muss das SMGW tagesgenaue Zählerstände für alle vom SMGW im Rahmen der abrechnungsrelevanten Tarifierung erfassten Messgrößen vorhalten. Dies geschieht automatisch für jede im SMGW durch ein Auswertungsprofil erfasste oder erzeugte Messgröße. Somit ist dieser Anwendungsfall immer im Hintergrund aktiv. Die Daten dürfen jedoch nur in begründeten Ausnahmefällen abgerufen werden.

Das SMGW **MUSS** hierzu täglich zum Beginn des *abrechnungstechnischen Kalendertages* den aktuellen Zählerstand des Zählers erfassen und einen entsprechenden Eintrag in der zugehörigen Messwertliste erzeugen. [REQ.MWV.Taf6.10]

Der GWA kann im Auftrag eines EMT, der durch den Anschlussnutzer berechtigt wurde, den Versand von Messwerten im besonderen Bedarfsfall für einen bestimmten Stichtag veranlassen. Falls der Versand an den GWA erfolgt, gibt dieser die angefragten Messwerte an den EMT weiter.

Das SMGW **MUSS** die in diesem Anwendungsfall zu versendenden Daten vor der Inhaltsdatenverschlüsselung mit einer zusätzlichen Signatur versehen. [REQ.MWV.Taf6.20]

Das SMGW stellt dem Anschlussnutzer zu diesem Anwendungsfall Daten über die HAN-Schnittstelle bereit (s. ▶Abschnitt 4.2.4.4). Der jeweilige Anschlussnutzer wird über die Anschlussnutzerkennung identifiziert, die dem Zähler zugeordnet sein muss.

4.2.4.2. Notwendige Parameter für das Regelwerk

Es bestehen keine Vorgaben an notwendige Parameter für dieses Regelwerk.



ICS.MWV.Taf6Parameter.10

Der GWH **MUSS** im ICS beschreiben, ob und welche weitere Parametrierung notwendig ist, damit das SMGW Zählerstände gemäß ▶REQ.MWV.Taf6.10 erfasst (siehe auch ▶ICS.MWV.Auswertungsprofil.10).



ICS.MWV.Taf6Parameter.20

Der GWH **MUSS** im ICS beschreiben, wie der GWA bei Auslösung des Versands im Bedarfsfall den Stichtag, den berechtigten Empfänger und den Versandzeitpunkt festlegt.



ICS.MWV.Taf6Parameter.30

Der GWH **MUSS** im ICS beschreiben, wie die Berechtigung des Anschlussnutzers zum Zugriff auf die Tageswerte gemäß ▶Abschnitt 4.2.4.4 festgelegt wird.

4.2.4.3. Vom Regelwerk für EMT bereitzustellende Daten

- Das SMGW **MUSS** dem EMT für diesen TAF6 tagesgenaue Zählerstände und Stände der abgeleiteten Register zum angefragten Zeitpunkt innerhalb der letzten 6 Wochen bereitstellen. [REQ.MWV.Taf6EmtDaten.10]
- Das SMGW **MUSS** dem EMT für diesen TAF6 den Bezeichner des zugehörigen Auswertungsprofils bereitstellen. [REQ.MWV.Taf6EmtDaten.20]

4.2.4.4. Für den jeweiligen Anschlussnutzer an der HAN-Schnittstelle bereitzustellende Daten

- Das SMGW **MUSS** dem Anschlussnutzer an der HAN-Schnittstelle für diesen TAF6 die tagesgenauen Zählerstände seiner eigenen Zähler in den letzten 6 Wochen bereitstellen. [REQ.MWV.Taf6AnDaten.10]
- Das SMGW **MUSS** dem Anschlussnutzer an der HAN-Schnittstelle für diesen TAF6 die tagesgenauen Stände der ihm zugeordneten abgeleiteten Register in den letzten 6 Wochen bereitstellen. [REQ.MWV.Taf6AnDaten.20]
- Das SMGW **MUSS** dem Anschlussnutzer an der HAN-Schnittstelle für diesen TAF6 die Zeitpunkte, zu denen der GWA den Versand veranlasst hat, bereitstellen. [REQ.MWV.Taf6AnDaten.30]
- Weitere Daten gemäß den Anforderungen in ▶Abschnitt 3.4.2.1.

4.2.5. TAF7: Zählerstandsgangmessung

4.2.5.1. Beschreibung

Dieser Anwendungsfall erlaubt die Erfassung und Versendung von Zählerstandsgängen. Über diesen Anwendungsfall ist zudem eine zentrale Tarifierung durch den EMT möglich.

Das SMGW **MUSS** die Zählerstände im Takt der Registrierperiode erfassen und einen Eintrag in der zugehörigen Messwertliste erzeugen. [REQ.MWV.Taf7.10]

Zähler und Messgrößen werden über die Geräte-ID des Zählers und die OBIS-Kennzahlen der aufzuzeichnenden Messgrößen ausgewählt.

Das SMGW **MUSS** die Messwerte zu den definierten Versandzeitpunkten an berechnete EMT versenden. [REQ.MWV.Taf7.20] Über die parametrisierten Berechtigungen wird geregelt, welcher EMT berechnete ist.

Das SMGW **MUSS** die in diesem Anwendungsfall zu versendenden Daten vor der Inhaltsdatenverschlüsselung mit einer zusätzlichen Signatur versehen. [REQ.MWV.Taf7.30]

Das SMGW stellt dem Anschlussnutzer zu diesem Anwendungsfall Daten über die HAN-Schnittstelle bereit (s. ▶Abschnitt 4.2.5.4). Über eine Anschlussnutzererkennung ist der Tarif mit dem Anschlussnutzer verknüpft.

Das SMGW **MUSS** den Betrieb des Regelwerks zu Beginn des Gültigkeitszeitraums oder, falls der Beginn des Gültigkeitszeitraums in der Vergangenheit liegt, zum Zeitpunkt des Einspielens (sofern gemäß ▶ICS.MWV.Taf7Parameter.10 unterstützt) aufnehmen. [REQ.MWV.Taf7.40] Das SMGW **MUSS** den Betrieb des Regelwerks zum Ende des Gültigkeitszeitraums einstellen. [REQ.MWV.Taf7.50] Eine rückwirkende Tarifierung ist bei einem neu eingespielten Auswertungsprofil mit einem in der Vergangenheit liegenden Startzeitpunkt für den Gültigkeitszeitraum auszuschließen. Auch bei einer sofortigen Aufnahme des Betriebs des Regelwerks ist das Raster, das durch die Registrierperiode vorgegeben wird, einzuhalten (siehe *Sollregistrierzeitpunkt*).



Anmerkung

Der Anwendungsfall ermöglicht neben der Erfassung von Verbräuchen analog auch die Erfassung von Einspeisungen. In diesem Fall liefert der Zähler Messwerte für eingespeiste Energiemengen anstatt für verbrauchte Energiemengen.

4.2.5.2. Notwendige Parameter für das Regelwerk

Das SMGW **MUSS** die folgenden Parameter zur Parametrierung eines TAF7 akzeptieren: [REQ.MWV.Taf7Parameter.10]

Parameter	Beschreibung
Geräte-ID des Zählers	Der eindeutige Bezeichner des Zählers.
Liste von OBIS-Kennzahlen der zu registrierenden Messwerte	Die eindeutigen Kennzahlen der für den Tarif zu registrierenden Messgrößen des Zählers.
Zählpunktbezeichnung	Der eindeutige Bezeichner der Messlokation.
Registrierperiode	Der zeitliche Abstand zwischen zwei aufeinanderfolgenden Messwerterfassungen.
Abrechnungszeitraum	Der Zeitraum für den Zählerstände gemeinsam verschickt werden sollen (Blockbildung).
Anschlussnutzerkennung	Die eindeutige Kennung des Anschlussnutzers, der die angefallenen Daten einsehen darf.
Berechtigungen	Berechtigungen, die regeln, wer die ermittelten Daten über HAN oder WAN erhalten oder auslesen darf.
Versandzeitpunkte	Die Zeitpunkte zu denen die ermittelten Daten vom SMGW versendet werden.
Gültigkeitszeitraum	Der Zeitraum für den das Regelwerk im SMGW verwendet werden soll.

Tabelle 4.6 Regelwerkparameter für TAF7



ICS.MWV.Taf7Parameter.10

Der GWH **MUSS** im ICS angeben, ob das SMGW einen Zeitpunkt in der Vergangenheit für den Beginn des Gültigkeitszeitraums gemäß ▶REQ.MWV.Taf7.40 akzeptiert und den Betrieb des Regelwerks in diesem Fall zum Einspielzeitpunkt aufnimmt.

4.2.5.3. Vom Regelwerk für EMT bereitzustellende Daten

- Das SMGW **MUSS** dem EMT für diesen TAF7 den *Zählerstandsgang* für den Abrechnungszeitraum bereitstellen. [REQ.MWV.Taf7EmitDaten.10]
- Das SMGW **MUSS** dem EMT für diesen TAF7 den Bezeichner des zugehörigen Auswertungsprofils bereitstellen. [REQ.MWV.Taf7EmitDaten.20]

4.2.5.4. Für den jeweiligen Anschlussnutzer an der HAN-Schnittstelle bereitzustellende Daten

- Das SMGW **MUSS** dem Anschlussnutzer an der HAN-Schnittstelle für diesen TAF7 die Messwertliste bereitstellen. [REQ.MWV.Taf7AnDaten.10]
- Das SMGW **MUSS** dem Anschlussnutzer an der HAN-Schnittstelle für diesen TAF7 alle an EMT versendete Daten bereitstellen. [REQ.MWV.Taf7AnDaten.20]
- Weitere Daten gemäß den Anforderungen in ▶Abschnitt 3.4.2.1.

4.2.6. TAF9: Bereitstellung der Ist-Einspeisung einer Erzeugungsanlage

4.2.6.1. Beschreibung

Dieser Anwendungsfall erlaubt die Bereitstellung der Ist-Einspeiseleistung nach dem Erneuerbare-Energiengesetz und dem Kraft-Wärme-Kopplungsgesetz.

Das SMGW muss periodisch, bei Bedarf auf Verlangen des berechtigten Empfängers (ausgelöst durch den GWA) oder bei Eintritt bestimmter Ereignisse ausgewählte Werte an die berechtigten Empfänger übermitteln.

Das SMGW **KANN** Einspeisewerte aggregieren (z.B. Maximum-, Minimum- und Mittelwertbildung). [REQ.MWV.Taf9.10]

Wenn die Option für die Bildung von *aggregierten Werten* im SMGW implementiert und auch parametrierbar wurde, **MUSS** das SMGW die aggregierten Werte auf Basis der Momentanwerte und den Parametern für die Bildungsregeln und der *Aggregationsperiode* berechnen. [REQ.MWV.Taf9.20] Wenn die Option für die Bildung von aggregierten Werten im SMGW implementiert wurde, **MUSS** das SMGW zumindest eine Aggregationsperiode von 60 Sekunden unterstützen. [REQ.MWV.Taf9.30] Das SMGW **KANN** Aggregationsperioden kleiner oder größer als 60 Sekunden unterstützen. [REQ.MWV.Taf9.40]

Das SMGW muss die folgenden auslösenden Ereignisse für die Bereitstellung der *Ist-Einspeisung* unterstützen:

- Das SMGW **MUSS** den einmaligen Versand im Bedarfsfall unterstützen. [REQ.MWV.Taf9.50]
- Das SMGW **MUSS** den periodischen Versand unterstützen. [REQ.MWV.Taf9.60]
- Das SMGW **MUSS** den einmaligen Versand bei Überschreiten eines Schwellwerts durch einen Momentanwert oder einen aggregierten Wert unterstützen. [REQ.MWV.Taf9.70]
- Das SMGW **MUSS** den einmaligen Versand bei Unterschreiten eines Schwellwerts durch einen Momentanwert oder einen aggregierten Wert unterstützen. [REQ.MWV.Taf9.80]

Im Bedarfsfall **MUSS** das SMGW Momentanwerte oder aggregierte Werte (sofern nach ▶ICS.MWV.Taf9Aggregation.10 implementiert) an die berechtigten Empfänger versenden, sobald der GWA den einmaligen Versand auslöst. [REQ.MWV.Taf9.90]

Wenn die periodische Versendung parametrierbar wurde, **MUSS** das SMGW regelmäßig, unter Berücksichtigung der parametrierbaren Versandperiode, die Momentanwerte oder aggregierten Werte (sofern nach ▶ICS.MWV.Taf9Aggregation.10 implementiert) versenden. [REQ.MWV.Taf9.100] Das SMGW **MUSS** Versandperioden von 60 Sekunden unterstützen. [REQ.MWV.Taf9.110] Das SMGW **KANN** Versandperioden kleiner oder größer als 60 Sekunden unterstützen. [REQ.MWV.Taf9.120]

Sofern Schwellwerte parametrierbar wurden, **MUSS** das SMGW bei Über- oder Unterschreitung eines Schwellwerts die Momentanwerte oder aggregierten Werte (sofern nach ▶ICS.MWV.Taf9Aggregation.10 implementiert) versenden. [REQ.MWV.Taf9.130] Beim Versand aufgrund einer Schwellwertunterschreitung oder -überschreitung **MUSS** das SMGW sicherstellen, dass erkennbar ist, welche der übermittelten Messwerte für den Messwertversand verantwortlich sind. [REQ.MWV.Taf9.140]

Die Blockgröße ist der Zeitraum, über den Messwerte gemeinsam übertragen werden. Abhängig vom Parameter Blockgröße, **MUSS** das SMGW Werte entweder als Einzelwerte oder gesammelt als Block versenden. [REQ.MWV.Taf9.150]

Für die Erfassung von Momentanwerten sowie die *Aggregation* von Momentanwerten (sofern nach ▶ICS.MWV.Taf9Aggregation.10 implementiert) **MUSS** das SMGW eine Empfangsperiode von 60 Sekunden unterstützen. [REQ.MWV.Taf9.160] Das SMGW **KANN** kleinere oder größere Empfangsperioden unterstützen. [REQ.MWV.Taf9.170]

Zähler und Messgrößen der Einspeisewerte werden über die Geräte-ID des Zählers und die OBIS-Kennzahlen der Messgrößen ausgewählt. Das SMGW **MUSS** für diesen Anwendungsfall die Messgrößen in ▶Tabelle 4.7 unterstützen. [REQ.MWV.Taf9.180] Weitere Messgrößen **DARF** das SMGW **NICHT** unterstützen. [REQ.MWV.Taf9.190]

Das SMGW **MUSS** den Anschlussnutzer über einen Eintrag im Anschlussnutzer-Log informieren, wenn ein Versand von Messwerten im Bedarfsfall (einmaliger Abruf) stattgefunden hat und die berechtigten Empfänger der Messwerte dabei dokumentieren. [REQ.MWV.Taf9.200] Es werden keine Messwerte in das Anschlussnutzer-Log übernommen. Das SMGW **MUSS** den GWA über fehlgeschlagene Versandaufgaben per Event oder Logeintrag im System-Log informieren [REQ.MWV.Taf9.210]

Das SMGW stellt dem Anschlussnutzer zu diesem Anwendungsfall Daten über die HAN-Schnittstelle bereit (s. ▶Abschnitt 4.2.6.5). Der jeweilige Anschlussnutzer wird über die Anschlussnutzertennung identifiziert, die über das Auswertungsprofil, dem Zähler zugeordnet sein muss. Für den periodischen Versand sowie den einmaligen Versand aufgrund Unter- oder Überschreitung eines Schwellwerts werden keine ereignisbezogenen Einträge im Anschlussnutzer-Log erzeugt. In diesen Fällen wird der Anschlussnutzer über die Bereitstellung der Parameter des Regelwerks an der HAN-Schnittstelle über die Konfiguration des TAF 9 informiert.

Eine Messwertliste wird für diesen Anwendungsfall nicht angelegt. Die Daten, die bezüglich dieses Anwendungsfalls erhoben werden, sind nicht abrechnungsrelevant.



ICS.MWV.Taf9Aggregation.10

Der GWH **MUSS** im ICS angeben, ob das SMGW die Aggregation von Einspeisewerten gemäß ▶REQ.MWV.Taf9.10 unterstützt.



ICS.MWV.Taf9Aggregation.20

Der GWH **MUSS** im ICS angeben, welche Aggregationsperioden das SMGW gemäß ▶REQ.MWV.Taf9.40 zusätzlich unterstützt (s. ▶ICS.MWV.Taf9Aggregation.10).



ICS.MWV.Taf9Versand.10

Der GWH **MUSS** im ICS angeben, welche Versandperioden das SMGW gemäß ▶REQ.MWV.Taf9.120 zusätzlich unterstützt.



ICS.MWV.Taf9Empfangsperiode.10

Der GWH **MUSS** im ICS angeben, welche Empfangsperioden das SMGW gemäß ▶REQ.MWV.Taf9.170 zusätzlich unterstützt.

4.2.6.2. OBIS-Kennzahlen

OBIS-Kennzahl	Messgröße
1-0:36.7.0.255	Momentan-Wirkleistung P_{L1}
1-0:56.7.0.255	Momentan-Wirkleistung P_{L2}
1-0:76.7.0.255	Momentan-Wirkleistung P_{L3}
1-0:16.7.0.255	Momentan-Wirkleistung P_{ges}

Tabelle 4.7 Zugelassene Messgrößen aus dem Zähler für TAF9

4.2.6.3. Notwendige Parameter für das Regelwerk

Das SMGW **MUSS** die folgenden Parameter zur Parametrierung eines TAF9 akzeptieren: [REQ.MWV.Taf9Parameter.10]

Parameter	Beschreibung
Geräte-ID des Zählers	Der eindeutige Bezeichner des Zählers.

Parameter	Beschreibung
Liste von OBIS-Kennzahlen der zu verwendenden Messgrößen nach ▶Tabelle 4.4	Die eindeutige Kennzahl der für den Tarif zu verwendenden Messgröße des Zählers.
Zählpunktbezeichnung	Der eindeutige Bezeichner der Messlokation.
Empfangsperiode	Der zeitliche Abstand in dem Messwerte für diesen TAF von einem Zähler abgefragt beziehungsweise empfangen werden.
Anschlussnutzerkennung	Die eindeutige Kennung des Anschlussnutzers, der über die Versendung von Messwerten informiert wird. Hier der Anlagenbetreiber.
Berechtigungen	Berechtigungen, die regeln, wer die ermittelten Daten über HAN oder WAN erhalten oder auslesen darf.
Blockgröße	Der Zeitraum, über den die letzten Momentanwerte bzw. aggregierten Werte gemeinsam versendet werden sollen. Bei einer Blocklänge, die der Empfangsperiode entspricht, werden lediglich die zum Versandzeitpunkt aktuellen Momentanwerte bzw. die zuletzt aggregierten Werte versendet.
Gültigkeitszeitraum	Der Zeitraum für den das Regelwerk im SMGW verwendet werden soll.
Die Nutzung der folgenden Parameter im Auswertungsprofil ist optional.	
Versandperiode	Die Länge der Versandperiode.
Schwellwerte	Ein oder mehrere Schwellwerte, auf welche die Messwerte überprüft werden sollen.
Bildungsregeln für Aggregation ⁴	Bildungsregeln für die Aggregation von Momentanwerten.
Aggregationsperiode ⁴	Der Zeitraum, über den die Momentanwerte aggregiert werden sollen.

Tabelle 4.8 Regelwerkparameter für TAF9

**ICS.MWV.Taf9Parameter.10**

Der GWH **MUSS** im ICS angeben, ob das SMGW einen Zeitpunkt in der Vergangenheit für den Beginn des Gültigkeitszeitraums akzeptiert und den Betrieb des Regelwerks in diesem Fall zum Einspielzeitpunkt aufnimmt.

4.2.6.4. Vom Regelwerk für EMT bereitzustellende Daten

- Das SMGW **MUSS** dem EMT für diesen TAF9 die Momentanwerte der Ist-Einspeisung der Erzeugungsanlage oder aggregierte Werte bereitstellen. [REQ.MWV.Taf9EmtDaten.10]
- Das SMGW **MUSS** dem EMT für diesen TAF9 den Bezeichner des zugehörigen Auswertungsprofils bereitstellen. [REQ.MWV.Taf9EmtDaten.20]

4.2.6.5. Für den jeweiligen Anschlussnutzer an der HAN-Schnittstelle bereitzustellende Daten

- Das SMGW **MUSS** dem Anschlussnutzer an der HAN-Schnittstelle für diesen TAF9 die aktuellen Momentanwerte der Ist-Einspeisung der Erzeugungsanlage (in Abhängigkeit der Empfangsperiode) bereitstellen. [REQ.MWV.Taf9AnDaten.10]
- Das SMGW **MUSS** dem Anschlussnutzer an der HAN-Schnittstelle für diesen TAF9 das Anschlussnutzer-Log mit Informationen über den Versandzeitpunkt und die Identifikation des Empfängers bei jedem Versand von Messwerten im Bedarfsfall an einen berechtigten Empfänger bereitstellen. [REQ.MWV.Taf9AnDaten.20]

⁴ Sofern die Aggregation gemäß ▶ICS.MWV.Taf9Aggregation.10 vom SMGW implementiert wird.

4.2.7. TAF10: Abruf von Netzzustandsdaten

4.2.7.1. Beschreibung

Dieser Anwendungsfall ermöglicht die Bereitstellung von Netzzustandsdaten aus dem SMGW an den Netzbetreiber.

Das SMGW **MUSS** periodisch, bei Bedarf auf Verlangen (über den GWA) oder bei Eintritt bestimmter Ereignisse die Werte an den Netzbetreiber übermitteln. [REQ.MWV.Taf10.10] Sofern es aufgrund gesetzlicher Regelungen erforderlich ist, können Netzzustandsdaten pseudonymisiert werden (s. ▶Abschnitt 4.3.8).

Das SMGW **KANN** Netzzustandsdaten aggregieren (z.B. Maximum-, Minimum- und Mittelwertbildung). [REQ.MWV.Taf10.20] Die Bildungsregeln für die Aggregation von Netzzustandswerten sind dann entsprechend parametrierbar.

Wenn die Option für die Bildung von aggregierten Werten im SMGW implementiert und auch parametrierbar wurde, **MUSS** das SMGW die aggregierten Werte auf Basis der Momentanwerte und den Parametern für die Bildungsregeln und der Aggregationsperiode berechnen. [REQ.MWV.Taf10.30] Das SMGW **MUSS** zumindest eine Aggregationsperiode von 60 Sekunden unterstützen. [REQ.MWV.Taf10.40] Das SMGW **KANN** Aggregationsperioden kleiner oder größer als 60 Sekunden unterstützen. [REQ.MWV.Taf10.50]

Das SMGW muss die folgenden auslösenden Ereignisse für die Bereitstellung der Netzzustandsdaten unterstützen:

- Das SMGW **MUSS** den einmaligen Versand im Bedarfsfall unterstützen. [REQ.MWV.Taf10.60]
- Das SMGW **MUSS** den periodischen Versand unterstützen. [REQ.MWV.Taf10.70]
- Das SMGW **MUSS** den einmaligen Versand bei Überschreiten eines Schwellwerts durch einen Momentanwert oder einen aggregierten Wert unterstützen. [REQ.MWV.Taf10.80]
- Das SMGW **MUSS** den einmaligen Versand bei Unterschreiten eines Schwellwerts durch einen Momentanwert oder einen aggregierten Wert unterstützen. [REQ.MWV.Taf10.90]

Im Bedarfsfall **MUSS** das SMGW Momentanwerte oder aggregierten Werte (sofern nach ▶ICS.MWV.Taf10Aggregation.10 implementiert) an die berechtigten Empfänger versenden, sobald der GWA den einmaligen Versand auslöst. [REQ.MWV.Taf10.100]

Wenn die periodische Versendung parametrierbar wurde, **MUSS** das SMGW regelmäßig, unter Berücksichtigung der parametrierbaren Versandperiode, die Momentanwerte oder aggregierten Werte (sofern nach ▶ICS.MWV.Taf10Aggregation.10 implementiert) versenden. [REQ.MWV.Taf10.110] Das SMGW **MUSS** Versandperioden von 60 Sekunden unterstützen. [REQ.MWV.Taf10.120] Das SMGW **KANN** Versandperioden kleiner oder größer 60 Sekunden unterstützen. [REQ.MWV.Taf10.130]

Sofern Schwellwerte parametrierbar wurden, **MUSS** das SMGW bei Über- oder Unterschreitung eines Schwellwerts die Momentanwerte oder aggregierten Werte (sofern nach ▶ICS.MWV.Taf10Aggregation.10 implementiert) versenden. [REQ.MWV.Taf10.140] Beim Versand aufgrund einer Schwellwertunterschreitung oder -überschreitung **MUSS** das SMGW sicherstellen, dass erkennbar ist, welche der übermittelten Messwerte für den Messwertversand verantwortlich sind. [REQ.MWV.Taf10.150]

Die Blockgröße ist der Zeitraum, über den Messwerte gemeinsam übertragen werden. Abhängig vom Parameter Blockgröße, **MUSS** das SMGW Werte entweder als Einzelwerte oder gesammelt als Block versenden. [REQ.MWV.Taf10.160]

Für die Erfassung von Momentanwerten sowie die Aggregation von Momentanwerten (sofern nach ▶ICS.MWV.Taf10Aggregation.10 implementiert) **MUSS** das SMGW eine Empfangsperiode von 60 Sekunden unterstützen. [REQ.MWV.Taf10.170] Das SMGW **KANN** kleinere oder größere Empfangsperioden unterstützen. [REQ.MWV.Taf10.180]

Zähler und Messgrößen der Netzzustandsdaten werden über die Geräte-ID des Zählers und die OBIS-Kennzahlen der Messgrößen ausgewählt. Das SMGW **MUSS** für diesen Anwendungsfall die Messgrößen in ▶Tabel-

le 4.9 unterstützen. [REQ.MWV.Taf10.190] Weitere Messgrößen **DARF** das SMGW **NICHT** unterstützen. [REQ.MWV.Taf10.200]

Das SMGW **MUSS** den Anschlussnutzer über einen Eintrag im Anschlussnutzer-Log informieren, wenn ein Versand von Messwerten im Bedarfsfall (einmaliger Abruf) stattgefunden hat. [REQ.MWV.Taf10.210] Die berechtigten Empfänger der Messwerte werden dabei dokumentiert. Es werden keine Messwerte in das Anschlussnutzer-Log übernommen. Das SMGW **MUSS** den GWA über fehlgeschlagene Versandaufgaben per Event oder Logeintrag im System-Log informieren [REQ.MWV.Taf10.220]

Das SMGW stellt dem Anschlussnutzer zu diesem Anwendungsfall Daten über die HAN-Schnittstelle bereit (s. ▶Abschnitt 4.2.7.5). Der jeweilige Anschlussnutzer wird über die Anschlussnutzerkennung identifiziert, die über das Auswertungsprofil, dem Zähler zugeordnet sein muss. Für den periodischen Versand sowie den einmaligen Versand aufgrund Unter- oder Überschreitung eines Schwellwerts werden keine ereignisbezogenen Einträge im Anschlussnutzer-Log erzeugt. In diesen Fällen wird der Anschlussnutzer über die Bereitstellung der Parameter des Regelwerks an der HAN Schnittstelle über die Konfiguration des TAF 10 informiert.

Eine Messwertliste wird für diesen Anwendungsfall nicht angelegt. Die Daten, die bezüglich dieses Anwendungsfalls erhoben werden, sind nicht abrechnungsrelevant.



ICS.MWV.Taf10Aggregation.10

Der GWH **MUSS** im ICS angeben, ob das SMGW die Aggregation von Netzzustandsdaten gemäß ▶REQ.MWV.Taf10.20 unterstützt.



ICS.MWV.Taf10Aggregation.20

Der GWH **MUSS** im ICS angeben, welche Aggregationsperioden das SMGW gemäß ▶REQ.MWV.Taf10.50 zusätzlich unterstützt (s. ▶ICS.MWV.Taf10Aggregation.10).



ICS.MWV.Taf10Versand.10

Der GWH **MUSS** im ICS angeben, welche Versandperioden das SMGW gemäß ▶REQ.MWV.Taf10.130 zusätzlich unterstützt.



ICS.MWV.Taf10Empfangsperiode.10

Der GWH **MUSS** im ICS angeben, welche Empfangsperioden das SMGW gemäß ▶REQ.MWV.Taf10.180 zusätzlich unterstützt.

4.2.7.2. OBIS-Kennzahlen

OBIS-Kennzahl	Messgröße
1-0:36.7.0.255	Momentan-Wirkleistung P_{L1}
1-0:56.7.0.255	Momentan-Wirkleistung P_{L2}
1-0:76.7.0.255	Momentan-Wirkleistung P_{L3}
1-0:16.7.0.255	Momentan-Wirkleistung P_{ges}
1-0:31.7.0.255	Strommesswert zu L1
1-0:51.7.0.255	Strommesswert zu L2
1-0:71.7.0.255	Strommesswert zu L3
1-0:14.7.0.255	Frequenz
1-0:81.7.1.255	Phasenwinkel U-L2 zu U-L1

OBIS-Kennzahl	Messgröße
1-0:81.7.2.255	Phasenwinkel U-L3 zu U-L1
1-0:81.7.4.255	Phasenwinkel I-L1 zu U-L1
1-0:81.7.15.255	Phasenwinkel I-L2 zu U-L2
1-0:81.7.26.255	Phasenwinkel I-L3 zu U-L3
1-0:32.7.0.255	Spannungsmesswert zu L1
1-0:52.7.0.255	Spannungsmesswert zu L2
1-0:72.7.0.255	Spannungsmesswert zu L3

Tabelle 4.9 Zugelassene Messgrößen aus dem Zähler für TAF10

4.2.7.3. Notwendige Parameter für das Regelwerk

Das SMGW **MUSS** die folgenden Parameter zur Parametrierung eines TAF10 akzeptieren: [REQ.M-WV.Taf10Parameter.10]

Parameter	Beschreibung
Geräte-ID des Zählers	Der eindeutige Bezeichner des Zählers.
Liste von OBIS-Kennzahlen der zu verwendenden Messgrößen nach ►Tabelle 4.9	Die eindeutigen Kennzahlen der als Netzzustandsdaten zu verwendenden Messgrößen des Zählers.
Zählpunktbezeichnung	Der eindeutige Bezeichner der Messlokation.
Empfangsperiode	Der zeitliche Abstand in dem Messwerte für diesen TAF von einem Zähler abgefragt beziehungsweise empfangen werden.
Anschlussnutzerkennung	Die eindeutige Kennung des Anschlussnutzers, der über die Versendung von Messwerten informiert wird
Berechtigungen	Berechtigungen, die regeln, wer die ermittelten Daten erhalten darf.
Blockgröße	Der Zeitraum, über den die letzten Momentanwerte bzw. aggregierten Werte gemeinsam versendet werden sollen. Bei einer Blocklänge, die der Empfangsperiode entspricht, werden lediglich die zum Versandzeitpunkt aktuellen Momentanwerte bzw. die zuletzt aggregierten Werte versendet.
Gültigkeitszeitraum	Der Zeitraum für den das Regelwerk im SMGW verwendet werden soll.
Die Nutzung der folgenden Parameter im Auswertungsprofil ist optional.	
Versandperiode	Die Länge der Versandperiode.
Schwellwerte	Ein oder mehrere Schwellwerte, auf welche die Messwerte überprüft werden sollen.
Bildungsregeln für Aggregation ⁵	Bildungsregeln für die Aggregation von Momentanwerten.
Aggregationsperiode ⁵	Der Zeitraum, über den die Momentanwerte aggregiert werden sollen.
Pseudonym	Pseudonym, welches bei der Versendung der Netzzustandsdaten anstatt der Geräte-ID des Zählers versendet werden muss. Das Pseudonym wird vom GWA vorgegeben.

Tabelle 4.10 Regelwerkparameter für TAF10



ICS.MWV.Taf10Parameter.10

Der GWH **MUSS** im ICS angeben, ob das SMGW einen Zeitpunkt in der Vergangenheit für den Beginn des Gültigkeitszeitraums akzeptiert und den Betrieb des Regelwerks in diesem Fall zum Einspielzeitpunkt aufnimmt.

⁵ Sofern die Aggregation gemäß ►ICS.MWV.Taf10Aggregation.10 vom SMGW implementiert wird.

4.2.7.4. Vom Regelwerk für EMT bereitzustellende Daten

- Das SMGW **MUSS** dem EMT für diesen TAF10 Momentanwerte oder aggregierte Werte der netzzustandsrelevanten Messgrößen bereitstellen. [REQ.MWV.Taf10EmtDaten.10]
- Das SMGW **MUSS** dem EMT für diesen TAF10 den Bezeichner des zugehörigen Auswertungsprofils bereitstellen. [REQ.MWV.Taf10EmtDaten.20]

4.2.7.5. Für den jeweiligen Anschlussnutzer an der HAN-Schnittstelle bereitzustellende Daten

- Das SMGW **MUSS** dem Anschlussnutzer an der HAN-Schnittstelle für diesen TAF10 das Anschlussnutzer-Log mit Informationen über den Versandzeitpunkt und die Identifikation des Empfängers bei jedem Versand von Messwerten im Bedarfsfall an einen berechtigten Empfänger bereitstellen. [REQ.MWV.Taf10AnDaten.10]

4.2.8. TAF14: Hochfrequente Messwertbereitstellung für Mehrwertdienste

4.2.8.1. Beschreibung

Dieser Anwendungsfall erlaubt die hochfrequente Bereitstellung von Messwerten als Grundlage zur Umsetzung von Mehrwertdiensten (z.B. die Visualisierung der Messwerte für den Anschlussnutzer durch ein Internetportal).

Das SMGW **MUSS** periodisch oder direkt bei Eingang im SMGW ausgewählte Werte an die berechtigten Empfänger übermitteln. [REQ.MWV.Taf14.10] Berechtigte Empfänger sind grundsätzlich alle Marktteilnehmer (z.B. Lieferanten, Direktvermarkter und Aggregatoren), die über eine Einwilligung des Anschlussnutzers für die jeweilige Datenerhebung verfügen. Die Auswahl wird durch den GWA über das entsprechende Auswertungsprofil vorgegeben.

Das SMGW muss die folgenden auslösenden Ereignisse für die Bereitstellung der unten genannten Messwerte unterstützen:

- Das SMGW **MUSS** einen periodischen Versand unterstützen. [REQ.MWV.Taf14.20]
- Das SMGW **MUSS** einen Ad-hoc Versand beim Eingang eines neuen Messwerts unterstützen. [REQ.MWV.Taf14.30]
- Das SMGW **MUSS** einen einmaligen Versand bei Überschreiten eines Schwellwerts durch einen Messwert unterstützen. [REQ.MWV.Taf14.40]
- Das SMGW **MUSS** einen einmaligen Versand bei Unterschreiten eines Schwellwerts durch einen Messwert unterstützen. [REQ.MWV.Taf14.50]

Wenn eine Versandperiode parametrierung wurde, **MUSS** das SMGW regelmäßig, unter Berücksichtigung der parametrierung Versandperiode, die seit dem letzten Versand erfassten Messwerte versenden. [REQ.MWV.Taf14.60] Das SMGW **MUSS** Versandperioden von 60 Sekunden unterstützen. [REQ.MWV.Taf14.70] Das SMGW **KANN** Versandperioden kleiner oder größer als 60 Sekunden unterstützen. [REQ.MWV.Taf14.80] Die Versandperiode bestimmt, wie viele Messwerte gemeinsam übermittelt werden. Sofern Schwellwerte parametrierung wurden, **SOLL** das SMGW bei Über- oder Unterschreitung eines Schwellwerts die seit dem letzten Versand erfassten Messwerte versenden. [REQ.MWV.Taf14.90] Dabei muss erkennbar sein, welche der übermittelten Messwerte für den Messwertversand verantwortlich sind.

Wenn keine Versandperiode und keine Schwellwerte parametrierung wurden, **MUSS** das SMGW jeden Messwert direkt bei seiner Registrierung im SMGW versenden. [REQ.MWV.Taf14.100]

Für die Erfassung von Messwerten **MUSS** das SMGW eine Empfangsperiode von 60 Sekunden unterstützen. [REQ.MWV.Taf14.110] Das SMGW **KANN** kleinere oder größere Empfangsperioden unterstützen. [REQ.MWV.Taf14.120]

Zähler und Messgrößen werden über die Geräte-ID des Zählers und die OBIS-Kennzahlen der Messgrößen ausgewählt. Das SMGW **MUSS** für diesen Anwendungsfall die Messgrößen in ▶Tabelle 4.11 unterstützen. [REQ.MWV.Taf14.130] Weitere Messgrößen **DARF** das SMGW unterstützen. [REQ.MWV.Taf14.140]

Das SMGW **MUSS** den Anschlussnutzer mit einem Eintrag im Anschlussnutzer-Log über die Parametrierung des Versands von Messwerten durch den TAF14 informieren. [REQ.MWV.Taf14.150] Es werden keine Messwerte in das Anschlussnutzer-Log übernommen.

Das SMGW stellt dem Anschlussnutzer zu diesem Anwendungsfall Daten über die HAN-Schnittstelle bereit (s. ▶Abschnitt 4.2.8.5). Der jeweilige Anschlussnutzer wird über die Anschlussnutzerkennung identifiziert, die über das Auswertungsprofil dem Zähler zugeordnet sein muss. Es werden keine ereignisbezogenen Einträge im Anschlussnutzer-Log erzeugt. Der Anschlussnutzer wird über die Bereitstellung der Parameter des Regelwerks an der HAN-Schnittstelle über die Konfiguration des TAF14 informiert.

Eine Messwertliste wird für diesen Anwendungsfall nicht angelegt. Die Daten, die bezüglich dieses Anwendungsfalls erhoben werden, sind nicht abrechnungsrelevant.



ICS.MWV.Taf14Versand.10

Der GWH **MUSS** im ICS angeben, welche Versandperioden das SMGW gemäß ▶REQ.MWV.Taf14.80 zusätzlich unterstützt.



ICS.MWV.Taf14Empfangsperiode.10

Der GWH **MUSS** im ICS angeben, welche Empfangsperioden das SMGW gemäß ▶REQ.MWV.Taf14.120 zusätzlich unterstützt.



ICS.MWV.Taf14Vorhaltung.10

Der GWH **MUSS** im ICS angeben, wie viele Werte oder welcher Zeitraum zwischen zwei Versandzeitpunkten gemäß ▶REQ.MWV.Taf14.90 mindestens vom SMGW vorgehalten und versendet werden können⁶.



ICS.MWV.Taf14Obis.10

Der GWH **MUSS** im ICS angeben, welche OBIS-Kennzahlen das SMGW gemäß ▶REQ.MWV.Taf14.140 zusätzlich unterstützt.

4.2.8.2. OBIS-Kennzahlen

OBIS-Kennzahl	Messgröße
1-0:1.8.0.255	Zählerstand zur Wirkarbeit in Richtung A+
1-0:21.8.0.255	Zählerstand zur Wirkarbeit in Richtung A+ L1
1-0:41.8.0.255	Zählerstand zur Wirkarbeit in Richtung A+ L2
1-0:61.8.0.255	Zählerstand zur Wirkarbeit in Richtung A+ L3
1-0:2.8.0.255	Zählerstand zur Wirkarbeit in Richtung A-
1-0:22.8.0.255	Zählerstand zur Wirkarbeit in Richtung A- L1
1-0:42.8.0.255	Zählerstand zur Wirkarbeit in Richtung A- L2
1-0:62.8.0.255	Zählerstand zur Wirkarbeit in Richtung A- L3

⁶ Hierbei ist zu bedenken, dass der periodische Versand deaktivierbar ist und zwei Versandzeitpunkte aufgrund von Schwellwertverletzungen weit auseinanderliegen können.

OBIS-Kennzahl	Messgröße
1-0:5.8.0.255	Zählerstand zur Blindarbeit in Richtung R1
1-0:6.8.0.255	Zählerstand zur Blindarbeit in Richtung R2
1-0:7.8.0.255	Zählerstand zur Blindarbeit in Richtung R3
1-0:8.8.0.255	Zählerstand zur Blindarbeit in Richtung R4
1-0:16.7.0.255	Momentan-Wirkleistung
1-0:36.7.0.255	Momentan-Wirkleistung P_{L1}
1-0:56.7.0.255	Momentan-Wirkleistung P_{L2}
1-0:76.7.0.255	Momentan-Wirkleistung P_{L3}

Tabelle 4.11 Zugelassene Messgrößen aus dem Zähler für TAF14

4.2.8.3. Notwendige Parameter für das Regelwerk

Das SMGW **MUSS** die folgenden Parameter zur Parametrierung eines TAF14 akzeptieren: [REQ.M-WV.Taf14Parameter.10]

Parameter	Beschreibung
Geräte-ID des Zählers	Der eindeutige Bezeichner des Zählers.
Liste von OBIS-Kennzahlen der zu verwendenden Messwerte	Die eindeutigen Kennzahlen der als Netzzustandsdaten zu verwendenden Messgrößen des Zählers.
Zählpunktbezeichnung	Der eindeutige Bezeichner der Messlokation.
Empfangsperiode	Der zeitliche Abstand in dem Messwerte für diesen TAF von einem Zähler abgefragt beziehungsweise empfangen werden.
Anschlussnutzerkennung	Die eindeutige Kennung des Anschlussnutzers, der über die Versendung von Messwerten informiert wird.
Berechtigungen	Berechtigungen, die regeln, wer die ermittelten Daten erhalten darf.
Gültigkeitszeitraum	Der Zeitraum, für den das Regelwerk im SMGW verwendet werden soll.
Die Nutzung der folgenden Parameter im Auswertungsprofil ist optional.	
Versandperiode	Die Länge der Versandperiode, sofern periodisch versendet werden soll. Im Falle einer ad-hoc Bereitstellung ist die Angabe dieses Parameters nicht erforderlich.
Schwellwerte	Ein oder mehrere Schwellwerte, auf welche die Messwerte überprüft werden sollen.

Tabelle 4.12 Regelwerkparameter für TAF14



ICS.MWV.Taf14Parameter.10

Der GWH **MUSS** im ICS angeben, ob das SMGW einen Zeitpunkt in der Vergangenheit für den Beginn des Gültigkeitszeitraums akzeptiert und den Betrieb des Regelwerks in diesem Fall zum Einspielzeitpunkt aufnimmt.

4.2.8.4. Vom Regelwerk für EMT bereitzustellende Daten

- Das SMGW **MUSS** dem EMT die erfassten Messwerte entsprechend den Vorgaben des Auswertungsprofils bereitstellen. [REQ.MWV.Taf14EmtDaten.10]
- Das SMGW **MUSS** dem EMT für diesen TAF14 den Bezeichner des zugehörigen Auswertungsprofils bereitstellen. [REQ.MWV.Taf14EmtDaten.20]

4.2.8.5. Für den jeweiligen Anschlussnutzer an der HAN-Schnittstelle bereitzustellende Daten

- Daten gemäß den Anforderungen in ▶Abschnitt 3.4.2.1.

4.3. Messwertverarbeitung mit Regelwerken

4.3.1. Konzeptübersicht

Das Konzept der Messwertverarbeitung ist in ▶Abbildung 4.4 dargestellt.

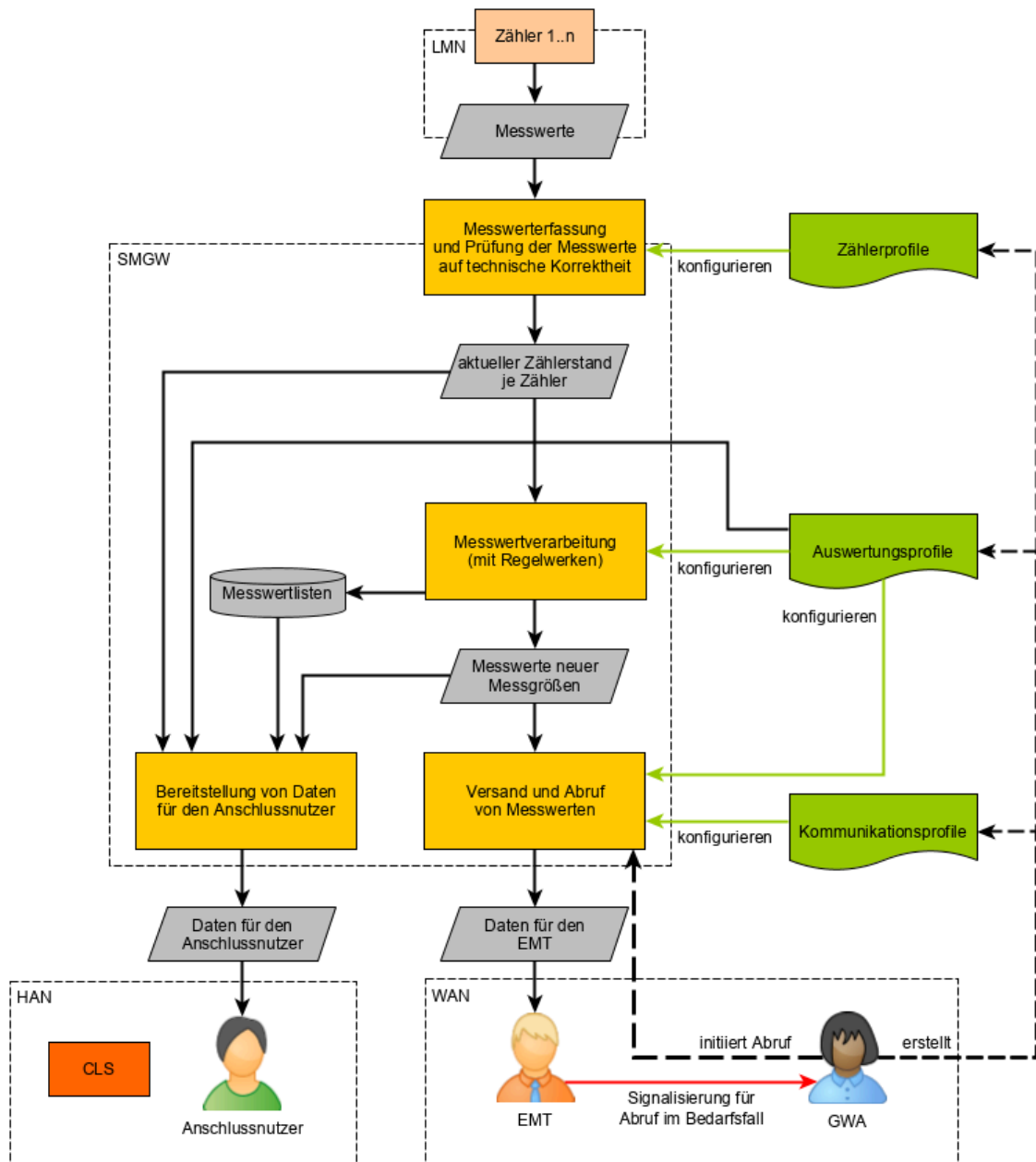


Abbildung 4.4. Übersicht der Messwertverarbeitung

Das SMGW erfasst *Messwerte* und *Statusinformationen* von verschiedenen Zählern, um diese in Regelwerken zu verarbeiten. Zu diesem Zweck verwaltet das SMGW jeden angeschlossenen Zähler und hält jeweils den zuletzt erfassten Wert als aktuellen Zählerstand des Zählers in seinem eigenen Speicher vor.

Entsprechend der konfigurierten Regelwerke werden originäre Messwerte in Messwertlisten abgelegt. Regelwerke verarbeiten die abgelegten *originären Messwerte* und speichern die Ergebnisse in *abgeleiteten Registern* bzw. in *abgeleiteten Wertelisten*, die dann für den Versand an EMT vorgehalten werden. Je nach Regelwerk erzeugt das SMGW für die Modellierung der verschiedenen Tarifstufen aus den Anwendungsfällen (s. ▶Abschnitt 4.2) ebenfalls abgeleitete Register. Das SMGW kann mehrere Regelwerke parallel betreiben, um Messwertverarbeitungen auch für mehrere Anschlussnutzer bzw. mehrere Anwendungsfälle durchführen zu können. Zu jedem abrechnungsrelevanten Regelwerk pflegt das SMGW eine gesonderte Messwertliste, in der die originären Messwerte der Zähler aufgezeichnet werden, die bei der Messwertverarbeitung im Regelwerk verwendet werden. Die Messwertliste dient dem Zweck, dass ein Anschlussnutzer seine Abrechnungen anhand der originären Messwerte der Zähler nachvollziehen kann. Jeder Anschlussnutzer kann dazu die ihm zugeordneten Messwertlisten und die Werte der abgeleiteten Register / Wertelisten über die Anzeigeeinheit (IF_GW_CON) einsehen (s. ▶Abschnitt 3.4.2.1).

Die Konfiguration sämtlicher Teilaspekte der Messwernerfassung und -verarbeitung obliegt dem GWA. Regelwerke werden über Auswertungsprofile konfiguriert, welche die Parameter für die verschiedenen Anwendungsfälle aus ▶Abschnitt 4.2 festlegen. Diese legen auch die Berechtigungen fest, die den EMT im WAN oder aber CLS im HAN (ggf. in der Rolle des Anschlussnutzers) Zugriff auf die abgeleiteten Register ermöglichen. Der Anschlussnutzer hat jederzeit die Möglichkeit, den aktuellen Stand und die bereits versendeten Werte, der für ihn relevanten abgeleiteten Register, über seine Anzeigeeinheit (IF_GW_CON) einzusehen.

Vom GWA eingebrachte WAN-Kommunikationsprofile legen fest, über welche TLS-Verbindung Messwerte an EMT im WAN versendet werden.

4.3.2. Messwernerfassung

Das SMGW **MUSS** Zählerstände von mehreren angeschlossenen Zählern erfassen können. [REQ.MWV.MwErfassung.10] Jeder Zähler muss über seine Geräte-ID im SMGW eindeutig identifizierbar und adressierbar sein. Bei dem Empfang von Zählerständen **MUSS** das SMGW die Sicherung der Kommunikation gemäß ▶Abschnitt 3.2.4 sicherstellen und das jeweilige Fachprotokoll nach ▶Abschnitt 3.3.5.1 auswerten. [REQ.MWV.MwErfassung.20] Die Konfiguration dazu muss vom GWA durch Zählerprofile (s. ▶Abschnitt 4.4.2) eingebracht werden können.

Das SMGW **MUSS** zu jedem angeschlossenen Zähler aktuelle Zählerstände der in einem Auswertungsprofil referenzierten Messgrößen vorhalten. [REQ.MWV.MwErfassung.30] Das SMGW **MUSS** dem GWA dazu die Konfiguration ermöglichen, welche Messgrößen des Zählers relevant sind und in Form von aktuellen Zählerständen im SMGW abgebildet werden müssen. [REQ.MWV.MwErfassung.40] Zu jedem Zählerstand **MUSS** das SMGW den Zeitstempel des Eingangs, die Statuszusatzinformationen des Zählers und das vom SMGW gebildete Statuswort ablegen. [REQ.MWV.MwErfassung.50] (s. ▶Abschnitt 4.3.4 und ▶Abschnitt 4.3.5).

Das SMGW **MUSS** Messwerte im 15-Minutentakt und im 60-Minutentakt registrieren können und mindestens in diesem Takt aktuelle Zählerstände von den Zählern vorhalten können. [REQ.MWV.MwErfassung.60]

Das SMGW **MUSS** bei der Erfassung von Messwerten technische Korrektheitsprüfungen durchführen, um zu entscheiden, ob ein Messwert gültig ist. [REQ.MWV.MwErfassung.70] Details zur Umsetzung der Korrektheitsprüfungen sind in ▶Abschnitt 4.3.4 zu finden.

Für die Identifizierung von Messgrößen der Zähler **MÜSSEN** OBIS-Kennzahlen gemäß [EN62056-6-1] bzw. [EN13757-1] verwendet werden. [REQ.MWV.MwErfassung.80]

Falls das SMGW die Messwerte über das [EN13757-3] Applikationsprotokoll empfängt, **MUSS** das SMGW zuvor eine Umsetzung in OBIS-Kennzahlen gemäß [EN13757-3] Annex H.2 und [OMSS4] Annex A durchführen. [REQ.MWV.MwErfassung.90]

Jedem Zähler muss der Anschlussnutzer zugeordnet werden, dessen Verbrauch oder Einspeisung er misst.

4.3.3. Messwertverarbeitung

Das SMGW **MUSS** auf Basis von Zählerständen der angeschlossenen Zähler *neue Messgrößen* bilden können. [REQ.MWV.MwVerarbeitung.10] Zu diesem Zweck **MÜSSEN** die Regelwerke des SMGW die abgeleiteten Register und abgeleiteten Wertelisten vorhalten. [REQ.MWV.MwVerarbeitung.20]

Die Konfiguration eines Regelwerks definiert, wie aus originären Zählerständen die Registerstände der abgeleiteten Register bzw. abgeleitete Wertelisten und die Messwertliste des Zählers gebildet werden. Die Konfiguration besteht aus einem Auswertungsprofil, welches das Regelwerk parametrisiert. Der Aufbau von Auswertungsprofilen ist in ▶Abschnitt 4.4.3 beschrieben.

Das SMGW **MUSS** abgeleitete Register für die Abbildung der verschiedenen Tarifstufen der Anwendungsfälle (s. ▶Abschnitt 4.2) verwenden. [REQ.MWV.MwVerarbeitung.30] Abgeleitete Wertelisten werden für die Abbildung der Ergebnisse der Messwertverarbeitung verwendet.

Das SMGW **MUSS** abgeleitete Register oder Wertelisten dem Anschlussnutzer zuordnen, für den die Auswertungen vorgenommen werden. [REQ.MWV.MwVerarbeitung.40] Die aktuellen und die bereits versendeten Werte der abgeleiteten Register oder Wertelisten müssen von dem zugehörigen Anschlussnutzer eingesehen werden können.

Zulässige Zugriffe auf die Messwerte werden in ▶Abschnitt 4.5 beschrieben.

Auch für die Identifizierung der Messgrößen in den abgeleiteten Registern und Wertelisten **MÜSSEN** OBIS-Kennzahlen verwendet werden [EN62056-6-1]. [REQ.MWV.MwVerarbeitung.50]

Das SMGW **MUSS** jeden originären Messwert eines Zählers, der im Regelwerk für die Messwertverarbeitung verwendet wird und gemäß [MessEG]/[MessEV] für die Bildung neuer abrechnungsrelevanter Messgrößen herangezogen wird, zusätzlich in einer Messwertliste ablegen. [REQ.MWV.MwVerarbeitung.60] Das SMGW **MUSS** zum Messwert außerdem den Zeitstempel der Erfassung und die Statuszusatzinformationen der technischen Korrektheitsprüfungen in der Messwertliste ablegen. [REQ.MWV.MwVerarbeitung.70]

Das SMGW **MUSS** Einträge in den Messwertlisten gemäß eichrechtlichen Vorgaben für mindestens 15 Monate aufbewahren. [REQ.MWV.MwVerarbeitung.80]

Das SMGW **MUSS** (ggf. im Zusammenwirken mit der Sichtanzeige nach [MessEG]/[MessEV] oder einem Dienst des MSB) die gesetzlichen Vorhaltefristen des [MsbG] erfüllen. [REQ.MWV.MwVerarbeitung.90]



ICS.MWV.MwVerarbeitung.10

Der GWH **MUSS** im ICS beschreiben, wie die Einhaltung der gesetzlichen Vorhaltefristen des [MsbG] gemäß ▶REQ.MWV.MwVerarbeitung.90 gewährleistet wird.

4.3.4. Verarbeitung von Statusinformationen

Bevor ein aus dem LMN versendeter Zählerstand zur weiteren Verarbeitung durch das SMGW verwendet werden darf, muss das SMGW prüfen, ob der gelieferte Messwert technisch korrekt ist und zur Abrechnung herangezogen werden darf. Dazu werden neben dem eigentlichen Zählerstand auch die vom Zähler versendeten Statusinformationen und der Betriebszustand des SMGW geprüft.

4.3.4.1. Prüfung der Messwerte auf technische Korrektheit

Empfängt das SMGW einen Messwert aus dem LMN, so **MUSS** das SMGW zunächst prüfen, ob der gelieferte Messwert Statusinformationen enthält, die nach [MessEG]/[MessEV] relevant sind. [REQ.MWV.MwStatus.10] Die Menge der nach [MessEG]/[MessEV] relevanten Statusinformationen, ist in ▶Tabelle 4.13 angegeben.⁷

Enthält der vom SMGW empfangene Messwert eine solche Statusinformation, so **MUSS** das SMGW die in ▶Tabelle 4.13 beschriebenen Aktionen durchführen. [REQ.MWV.MwStatus.20] Der empfangene Messwert **DARF**

⁷ Es dürfen nur solche Zähler für die Bildung und Änderung von abgeleiteten Registern verwendet werden, welche in der Lage sind, die in ▶Tabelle 4.13 aufgeführten Statusinformationen zu senden.

NICHT zur Bildung oder Veränderung von abgeleiteten Registern (ausgenommen Gesamtregister und Fehlerregister eines TAF2 nach ▶Abschnitt 4.2.3) durch das SMGW verwendet werden. [REQ.MWV.MwStatus.30]

Wenn das SMGW einen Messwert mit fatalem Fehler im Statuswort empfängt, **MUSS** das SMGW entweder alle zukünftig von diesem Zähler empfangenen Messwerte mit ebendiesem Statuswort markieren oder den Messbetrieb für diesen Zähler einstellen. [REQ.MWV.MwStatus.40]

Statuswort des Zählers	Bedeutung	Aktion durch das SMGW
Fataler Fehler	Gerät muss ausgetauscht werden.	Push-Meldung an den GWA. Erzeugung von Logmeldungen.

Tabelle 4.13 Abrechnungsrelevante Statusinformationen des Zählers

Zusätzlich **MUSS** das SMGW eigene Prüfungen durchführen, um festzustellen, ob der gelieferte Messwert technisch korrekt ist und ob der Betriebszustand des SMGW eine Bildung oder Änderung von abgeleiteten Registern zulässt. [REQ.MWV.MwStatus.50] Alle notwendigen Prüfungen, die mindestens vom SMGW durchgeführt werden **MÜSSEN**, sind in ▶Tabelle 4.14 beschrieben. [REQ.MWV.MwStatus.60] Zusätzlich können weitere Prüfungen durchgeführt werden.

Verläuft eine in ▶Tabelle 4.14 aufgeführte Prüfung negativ, so **MUSS** dies als Statusinformation des SMGW festgehalten werden und die entsprechenden Aktionen durch das SMGW ausgeführt werden (s. ▶Tabelle 4.14). [REQ.MWV.MwStatus.70] Der empfangene Messwert **DARF NICHT** zur Bildung oder Veränderung von abgeleiteten Registern (ausgenommen Gesamtregister und Fehlerregister eines TAF2 nach ▶Abschnitt 4.2.3) durch das SMGW verwendet werden. [REQ.MWV.MwStatus.80]

Prüfung	Statusinformation des SMGW, falls Prüfung negativ verläuft	Aktion durch das SMGW, falls Prüfung negativ verläuft
Liegt kein fataler Fehler im SMGW vor?	Fataler Fehler im SMGW.	Push-Meldung an den GWA. Erzeugung von Logmeldungen.
Ist die Zeit der Systemuhr korrekt?	Zeitinformation ist ungültig.	Erzeugung von Logmeldungen.

Tabelle 4.14 Technische Korrektheitsprüfungen, die vom SMGW durchzuführen sind

Das SMGW **MUSS** die Statusinformationen gemäß ▶Tabelle 4.13 oder ▶Tabelle 4.14 (diese liegen weiterhin als Rohdaten vor) im System-Log und im eichtechnischem Log speichern. [REQ.MWV.MwStatus.90] Außerdem **MUSS** das SMGW die Statusinformationen gemäß ▶Tabelle 4.13 oder ▶Tabelle 4.14 zusammen mit dem Zählerstand dem Anschlussnutzer an der HAN-Schnittstelle bereitstellen. [REQ.MWV.MwStatus.100] Dabei **DARF** das SMGW den Zählerstand **NICHT** an den GWA versenden oder im System-Log oder im eichtechnischen Log speichern. [REQ.MWV.MwStatus.110]



ICS.MWV.MwStatus.10

Der GWH **MUSS** im ICS angeben, ob das SMGW bei Auftreten eines fatalen Fehlers im Statuswort des Zählers den Messbetrieb für diesen Zähler gemäß ▶REQ.MWV.MwStatus.40 einstellt.

4.3.4.2. Weitere Prüfungen und Versand von Statusinformationen

Zusätzlich zu den in ▶Abschnitt 4.3.4.1 aufgeführten Prüfungen können auch anwendungsfallsspezifische Prüfverfahren angewandt werden. Dazu können die jeweiligen Prüfkriterien im Auswertungsprofil des zugehörigen Anwendungsfalls hinterlegt werden (s. ▶Abschnitt 4.4.3).⁸ In diesem Fall muss das Auswertungsprofil auch eine Beschreibung enthalten, wie im Fall einer negativ verlaufenden Prüfung zu verfahren ist.

⁸ Sind keine Prüfkriterien im Auswertungsprofil hinterlegt, so muss auch keine zusätzliche Prüfung durch das SMGW erfolgen. Die Tarifierung erfolgt in diesem Fall, wie im Auswertungsprofil beschrieben.

Bei einer entsprechenden Zweckbindung können im Bedarfsfall Statusinformationen, die vom einem Zähler im LMN an das SMGW gesendet werden, unter Verwendung des Anwendungsfalls TAF10: Abruf von Netzzustandsdaten (s. ▶Abschnitt 4.2.7) an autorisierte EMT übermittelt werden. Dabei muss sichergestellt werden, dass alle an EMT gesendeten Statusinformationen vom SMGW interpretiert werden können.

4.3.5. Zeitstempelung von Messwerten

Die Zeitpunkte der Erfassung von Zählerständen **MÜSSEN** im SMGW mithilfe der Systemzeit bestimmt werden. [REQ.MWV.MwZeitstempelung.10]

Wird von einem Zähler im LMN ein Messwert an das SMGW gesendet, so **MUSS** dieser Wert beim Eintreffen im SMGW mit einem Zeitstempel gemäß der Systemuhrzeit des SMGW versehen werden. [REQ.MWV.MwZeitstempelung.20] Nach erfolgreicher Korrektheitsprüfung (s. ▶Abschnitt 4.3.4) werden der Messwert und der zugehörige Zeitstempel als aktueller Zählerstand gespeichert. Somit ist jeder Zählerstand mit einem Zeitstempel versehen, der den Zeitpunkt des Eintreffens des Messwertes am Gateway angibt.

4.3.6. Übertragene Daten beim Messwertversand

Das SMGW **MUSS** beim Messwertversand sicherstellen, dass immer die folgenden Informationen enthalten sind: [REQ.MWV.MwVersand.10]

- Die Geräte-ID des Zählers (oder das Pseudonym).
- Der Zeitstempel der versendeten Messwerte.
- Die OBIS-Kennzahlen der Messwerte.
- Der abgeleitete Wert selbst.
- Die vorhandene Statusinformation (s. ▶Abschnitt 4.3.4).

Das SMGW **MUSS** die in ▶REQ.MWV.MwVersand.10 genannten Informationen auch dem zugehörigen Anschlussnutzer an der HAN-Schnittstelle bereitstellen. [REQ.MWV.MwVersand.20]

Die zu übertragenden Daten werden, wie in ▶Abschnitt 3.2.6.2 beschrieben, abgebildet.

4.3.7. Bereitstellung von Daten für den Anschlussnutzer

Das SMGW **MUSS** die empfangenen, gespeicherten und verarbeiteten Messwerte auch für die Visualisierung auf der Anzeigeeinheit des Anschlussnutzers bereitstellen. [REQ.MWV.AnDaten.10] Entsprechende Vorgaben sind je Anwendungsfall in ▶Abschnitt 4.2 genannt.

Das SMGW **MUSS** dem Anschlussnutzer die Möglichkeit bieten, einsehen zu können, wann welche Messwerte versendet worden sind. [REQ.MWV.AnDaten.20] Entsprechende Ereignisse **MUSS** das SMGW im zugehörigen Anschlussnutzer-Log hinterlegen. [REQ.MWV.AnDaten.30]

4.3.8. Pseudonymisierung/Anonymisierung

Der Anwendungsfall TAF10 gemäß ▶Abschnitt 4.2.7 sieht für den GWA die Möglichkeit vor, ein Pseudonym für den Messwertversand zu vergeben. Dadurch wird die Identität des Anschlussnutzers gegenüber dem EMT, der die Messwerte erhält, verschleiert. Sofern ein Pseudonym im Auswertungsprofil (▶Abschnitt 4.4.3) vorhanden ist, **MUSS** das SMGW die Identifikation des Zählers und des SMGW durch ein Pseudonym ersetzen. Die Identifikationen **DÜRFEN** in den (XML-) Inhaltsdaten **NICHT** mehr auftreten. [REQ.MWV.Pseudonymisierung.10]



Anmerkung

Netzwerkdiagnosedaten gemäß ▶Abschnitt 3.2.8 fallen nicht unter die Netzzustandsdaten nach § 2 [MsbG]. Eine Pseudonymisierung beim Versand von Netzwerkdiagnosedaten ist daher nicht erforderlich.

Die Pseudonymisierung von Netzzustandsdaten bei der Übertragung vom SMGW an einen EMT muss durch die folgenden Schritte sichergestellt werden:

1. Das SMGW **MUSS** aus Messwerten, die einem Auswertungsprofil folgend pseudonymisiert übertragen werden sollen, die Identifikation des Zählers und des SMGW entfernen und durch ein im Auswertungsprofil hinterlegtes Pseudonym ersetzen. [REQ.MWV.Pseudonymisierung.20]
2. Das SMGW **MUSS** die so aufbereiteten Daten entsprechend des konfigurierten WAN-Kommunikationsprofils dann für den Empfänger (EMT) verschlüsseln, signieren und an den GWA übertragen. [REQ.MWV.Pseudonymisierung.30]

Der GWA prüft die Signatur des SMGW und damit die Authentizität der empfangenen Daten und leitet diese nach Entfernung der SMGW Signatur an den Empfänger weiter.

3. Der Empfänger entschlüsselt die Nachricht.

4.4. Konfigurationsprofile

4.4.1. Einleitung

Die Konfiguration der Zähleranbindung, Messwernerfassung, -verarbeitung und -versand sowie der Kommunikation zu EMT im WAN wird über Konfigurationsprofile festgelegt, die vom GWA in das SMGW eingespielt werden.

▶Abbildung 4.5 stellt die Beziehungen zwischen den verschiedenen Profilen dar.

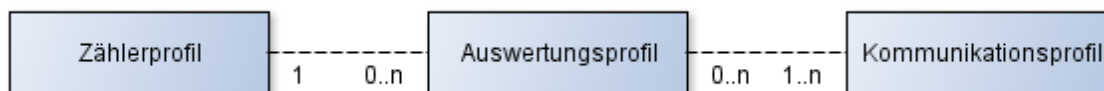


Abbildung 4.5. Beziehungen zwischen den Profilen für die Konfiguration der Tarifierung

Die Bedeutungen der verschiedenen Profile werden in den nächsten Abschnitten erläutert.

4.4.2. Zählerprofile

Ein Zählerprofil beschreibt die Konfiguration für das SMGW, die notwendig ist, um mit einem Zähler zu kommunizieren und die aktuellen Messwerte zu erfassen. Das SMGW **MUSS** die folgenden Parameter innerhalb des Zählerprofils akzeptieren: [REQ.MWV.Zählerprofil.10]

Parameter	Datentyp / Wertebereich ⁹	Beschreibung
Geräte-ID	Octet String	Der eindeutige Bezeichner des Zählers.
Kommunikationsszenario gemäß ▶Abschnitt 3.3.3	Einer aus: LKS1 LKS2	Legt das Kommunikationsszenario fest (s. ▶Abschnitt 3.3.3).
Kommunikationstyp	TLS Symmetrisch	Legt fest, ob TLS oder das symmetrische kryptographische Verfahren für die Sicherung der Kommunikation verwendet werden soll.

⁹ Die hier dargestellten Datentypen und Wertebereiche besitzen informativen Charakter.

Parameter	Datentyp / Wertebereich ⁹	Beschreibung
Protokoll		Das Protokoll für die Kommunikation mit dem Zähler. Hier wird der Protokolltreiber ausgewählt, der unter anderem dafür sorgt, dass die Messwerte nicht OBIS-fähige Zähler den relevanten OBIS-Kennzahlen zugeordnet werden.
Schlüsselmaterial	Symmetrischer Schlüssel	Der initiale symmetrische Schlüssel, der für die Absicherung der Kommunikation mit dem Zähler verwendet wird.
OBIS-Kennzahlen der Messgrößen	1..n Kennzahlen	Die Kennzahlen wählen die Messgrößen des Zählers aus, für die das SMGW die jeweils aktuellen Zählerstände speichern soll.

Tabelle 4.15 Parameter von Zählerprofilen

Das SMGW **KANN** weitere Parameter für Zählerprofile unterstützen. [REQ.MWV.Zählerprofil.20]

Zählerprofile werden über die *Geräte-ID* des jeweiligen Zählers in Auswertungsprofilen referenziert.

Zu der möglichen Modellierung der Datenstruktur der Zählerprofile siehe ▶Abschnitt 3.2.6.1.



ICS.MWV.Zählerprofil.10

Der GWH **MUSS** im ICS alle weiteren Parameter für Zählerprofile beschreiben, die gemäß ▶REQ.MWV.Zählerprofil.20 vom SMGW zusätzlich unterstützt werden.

4.4.3. Auswertungsprofile

Ein Auswertungsprofil parametrisiert ein Regelwerk, für einen konkreten Anwendungsfall. Das SMGW **MUSS** die folgenden Parameter innerhalb von Auswertungsprofilen akzeptieren: [REQ.MWV.Auswertungsprofil.10]

Parameter	Datentyp / Wertebereich ¹⁰	Beschreibung
Bezeichner	Alphanummerisch	Im SMGW eindeutiger Bezeichner für das Auswertungsprofil.
Name	Text	Ein Name für das Auswertungsprofil.
Auswahl des Anwendungsfalls	Nummer	Dieser Parameter legt den Anwendungsfall fest (aus ▶Abschnitt 4.2).
Alle für den jeweiligen Anwendungsfall notwendigen Parameter	Siehe entsprechenden Anwendungsfall in ▶Abschnitt 4.2.	Siehe entsprechenden Anwendungsfall in ▶Abschnitt 4.2.
Optional die vom SMGW durchzuführenden Prüfungen der Messwerte	-	Siehe ▶Abschnitt 4.3.4.
Zugeordnete WAN-Kommunikationsprofile	1..n Bezeichner	Die Bezeichner referenzieren die WAN-Kommunikationsprofile, die für den Versand von verarbeiteten Messwerten an EMT verwendet werden.

Tabelle 4.16 Durch Auswertungsprofile festzulegende Parameter eines Regelwerks

Das SMGW **KANN** weitere Parameter für Auswertungsprofile unterstützen. [REQ.MWV.Auswertungsprofil.20]

Zu der möglichen Modellierung der Datenstruktur der Auswertungsprofile siehe ▶Abschnitt 3.2.6.1.

Beim Einspielen des Auswertungsprofils muss das SMGW die folgenden Punkte sicherstellen:

⁹ Die hier dargestellten Datentypen und Wertebereiche besitzen informativen Charakter.

¹⁰ Die hier dargestellten Datentypen und Wertebereiche besitzen informativen Charakter.

- Das SMGW **MUSS** sicherstellen, dass die anhand der Geräte-ID referenzierten Zähler durch Zählerprofile konfiguriert sind. [REQ.MWV.Auswertungsprofil.30]
- Das SMGW **MUSS** sicherstellen, dass die im Auswertungsprofil angegebenen OBIS-Kennzahlen für Messgrößen auch im jeweiligen Zählerprofil hinterlegt sind. [REQ.MWV.Auswertungsprofil.40]
- Das SMGW **MUSS** sicherstellen, dass alle referenzierten WAN-Kommunikationsprofile im SMGW vorhanden sind. [REQ.MWV.Auswertungsprofil.50]
- Die verschiedenen Tarifstufen und Messwertlisten, die nach den Anwendungsfällen ausgewertet werden sollen, **MÜSSEN** im SMGW als abgeleitete Register oder abgeleitete Wertelisten persistiert werden können. [REQ.MWV.Auswertungsprofil.60]

Wird eine der genannten Prüfung nicht bestanden, so **DARF** das SMGW das Auswertungsprofil **NICHT** akzeptieren. [REQ.MWV.Auswertungsprofil.70] Das SMGW **MUSS** in diesem Fall einen entsprechenden Eintrag ins System-Log schreiben. [REQ.MWV.Auswertungsprofil.80]

Nach dem erfolgreichen Einspielen ist das Regelwerk konfiguriert und das SMGW **MUSS** unter Berücksichtigung des Gültigkeitszeitraums mit der Messwertverarbeitung beginnen. [REQ.MWV.Auswertungsprofil.90]



ICS.MWV.Auswertungsprofil.10

Der GWH **MUSS** im ICS alle weiteren Parameter für Auswertungsprofile beschreiben, die gemäß ▶REQ.MWV.Auswertungsprofil.20 vom SMGW zusätzlich unterstützt werden.

4.4.4. Kommunikationsprofile

Anforderungen an die jeweiligen Kommunikationsprofile sind an den folgenden Stellen beschrieben:

- WAN-Kommunikationsprofile in ▶Abschnitt 3.2.5.
- HAN-Kommunikationsprofile in ▶Abschnitt 3.4.5.2.
- Proxy-Kommunikationsprofil in ▶Abschnitt 3.4.5.3.

Die LMN-Kommunikation wird mittels Zählerprofil in ▶Abschnitt 4.4.2 parametrisiert.

4.5. Anforderungen an Berechtigungen

4.5.1. Einleitung

▶Abschnitt 4.5 klärt allgemeine Anforderungen an die Berechtigungen der verschiedenen Akteure des SMGW bezüglich Zugriff oder Erhalt von Daten.

4.5.2. Generelle Zugriffsbeschränkungen

- Das SMGW **MUSS** sicherstellen, dass kein geheimes Schlüsselmaterial aus dem SMGW ausgelesen werden kann. [REQ.WFA.GenerellerZugriff.10]
- Jede Zugriffsberechtigung muss zweckgebunden sein. Die Bewertung, ob ein Zugriff zweckgebunden ist oder nicht, wird in diesem Dokument nicht geklärt. Anforderungen hierzu könnten durch weitere Parteien aufgestellt werden.

4.5.3. Smart-Meter-Gateway-Administrator

- Der GWA muss alleinig die Berechtigungen haben, die Konfiguration und Administration des SMGW vorzunehmen. Dies betrifft insbesondere:

- Das SMGW **MUSS** sicherstellen, dass ausschließlich der GWA die Konfiguration für Messwerterfassung, Messwertverarbeitung und Versand von Messwerten und anderen Informationen an weitere EMT vornehmen kann. [REQ.WFA.GwaZugriff.10]
- Das SMGW **MUSS** sicherstellen, dass eine Einspielung von Firmware-Updates ausschließlich vom GWA veranlasst werden kann. [REQ.WFA.GwaZugriff.20]
- Das SMGW **MUSS** sicherstellen, dass ausschließlich der GWA eine Konfiguration zur Festlegung, welche EMT mit dem SMGW kommunizieren dürfen und welche Informationen diese über externe Schnittstellen erhalten dürfen, vornehmen kann. [REQ.WFA.GwaZugriff.30]
- Das SMGW **MUSS** sicherstellen, dass ausschließlich der GWA die Konfiguration des Sicherheitsmoduls vornehmen kann. [REQ.WFA.GwaZugriff.40]
- Das SMGW **MUSS** sicherstellen, dass ausschließlich der GWA die Konfiguration des Zertifikatsmaterials im SMGW vornehmen kann. [REQ.WFA.GwaZugriff.50]
- Das SMGW **MUSS** sicherstellen, dass der GWA die Messwertlisten nicht über das Kommunikationsszenario MANAGEMENT einsehen kann. [REQ.WFA.GwaZugriff.60]
- Das SMGW **MUSS** dem GWA die Möglichkeit bieten das Eichtechnische Log und das System-Log einsehen zu können. [REQ.WFA.GwaZugriff.70]
- Das SMGW **MUSS** sicherstellen, dass der GWA Einträge im Eichtechnischen Log und im System-Log nicht ändern kann. [REQ.WFA.GwaZugriff.80]
- Das SMGW **MUSS** sicherstellen, dass der GWA die Anschlussnutzer-Logs der Anschlussnutzer nicht einsehen oder ändern kann. [REQ.WFA.GwaZugriff.90]
- Das SMGW **MUSS** sicherstellen, dass der GWA als Einziger die Berechtigung hat, das SMGW über den Wake-Up-Service aufzuwecken. [REQ.WFA.GwaZugriff.100]

4.5.4. Servicetechniker

- Das SMGW **MUSS** dem Servicetechniker die Möglichkeit bieten, das System-Log des SMGW einzusehen. [REQ.WFA.SrvZugriff.10]
- Für den Zugriff auf weitere Diagnose-Informationen durch den Servicetechniker siehe Anwendungsfall HAF2 in ▶Abschnitt 3.4.2.2.
- Für den schreibenden Zugriff auf Kommunikationsparameter durch den Servicetechniker siehe Anwendungsfall HAF4 in ▶Abschnitt 3.4.2.4¹¹.

Das SMGW **MUSS** sicherstellen, dass der Servicetechniker keinen Zugriff auf Informationen erhält, für die keine Anforderung (REQ) bezüglich des Zugriffs durch den Servicetechniker existiert. [REQ.WFA.SrvZugriff.20] Das SMGW **MUSS** insbesondere sicherstellen, dass der Servicetechniker auf keine personenbeziehbaren Daten zugreifen kann. [REQ.WFA.SrvZugriff.30]

4.5.5. Anschlussnutzer

- Das SMGW **MUSS** dem Anschlussnutzer die Möglichkeit bieten, Auswertungsprofile (einschließlich aller Parameter des jeweiligen Regelwerks), Zählerstände und Messwertlisten, die für den Anschlussnutzer relevant sind, einzusehen. [REQ.WFA.AnZugriff.10]
- Für den Zugriff auf weitere Informationen durch den Anschlussnutzer siehe Anwendungsfall HAF1 in ▶Abschnitt 3.4.2.1.

Das SMGW **MUSS** sicherstellen, dass der Anschlussnutzer Daten, die nur andere Anschlussnutzer betreffen, nicht einsehen kann. [REQ.WFA.AnZugriff.20]

¹¹ Hierbei sind die Anforderungen gemäß [PP-0073] zu beachten. Änderungen dürfen keinen Einfluss auf die Sicherheitsfunktionalität haben.

4.5.6. Externe Marktteilnehmer

- Das SMGW **MUSS** sicherstellen, dass EMT ausschließlich Informationen vom SMGW erhalten, die durch Auswertungsprofile oder Netzwerkdiagnoseprofile vom GWA festgelegt worden sind. [REQ.WFA.EmtZugriff.10]
- Das SMGW **MUSS** sicherstellen, dass EMT keinen direkten Zugriff auf Messwertlisten haben, sondern Messwerte ausschließlich entsprechend der Berechtigungen der konfigurierten Auswertungsprofile (s. ▶ Abschnitt 4.2) vom SMGW an den EMT versendet werden. [REQ.WFA.EmtZugriff.20]

5. Weitere Funktionale Anforderungen

5.1. Zusammenspiel SMGW und Sicherheitsmodul

Neben den Protokollfestlegungen (s. ▶Kapitel 3) für die Übertragung von Daten zu Teilnehmern in den am SMGW angeschlossenen Netzen werden in ▶Kapitel 3 auch Maßnahmen zur Sicherung der Kommunikation auf Transport- und Inhaltsebene gefordert. Die dazu notwendigen kryptographischen Operationen zur Transport- und Inhaltsdatensicherung werden vom SMGW im Zusammenspiel mit seinem Sicherheitsmodul erbracht.

5.1.1. Nutzung des Sicherheitsmoduls beim TLS-Handshake

Das SMGW **MUSS** die Vorgaben an die Implementierung der kryptographischen Primitive von TLS aus [TR-03109-3] befolgen. [REQ.WFA.KryptoImplementierungTls.10] Dabei **MUSS** das SMGW mit einem Sicherheitsmodul zusammenarbeiten, das gemäß [PP-0077] zertifiziert wurde. [REQ.WFA.KryptoImplementierungTls.20]

Beim Aufbau des TLS-Kanals (Handshake) **MUSS** das SMGW sein Sicherheitsmodul einsetzen, wie in ▶Abbildung 5.1 und ▶Abbildung 5.2 beispielhaft dargestellt. [REQ.WFA.KryptoImplementierungTls.30] Folgende Funktionen des Sicherheitsmoduls müssen verwendet werden:

- Das SMGW **MUSS** das Sicherheitsmodul für die Generierung von Zufallszahlen für TLS-Kommando ClientHello verwenden. [REQ.WFA.KryptoImplementierungTls.40]
- Das SMGW **MUSS** das Sicherheitsmodul für die Schlüsselaushandlung des TLS pre-master secrets gemäß Elliptic Curve Diffie-Hellman verwenden. [REQ.WFA.KryptoImplementierungTls.50]
- Das SMGW **MUSS** das Sicherheitsmodul für die Signaturerzeugung und -prüfung für Authentifizierung verwenden. [REQ.WFA.KryptoImplementierungTls.60]

Das SMGW ist verantwortlich für die Generierung des *master secrets* und **MUSS** dazu das ausgehandelte *pre-master secret* verwenden. [REQ.WFA.KryptoImplementierungTls.70]

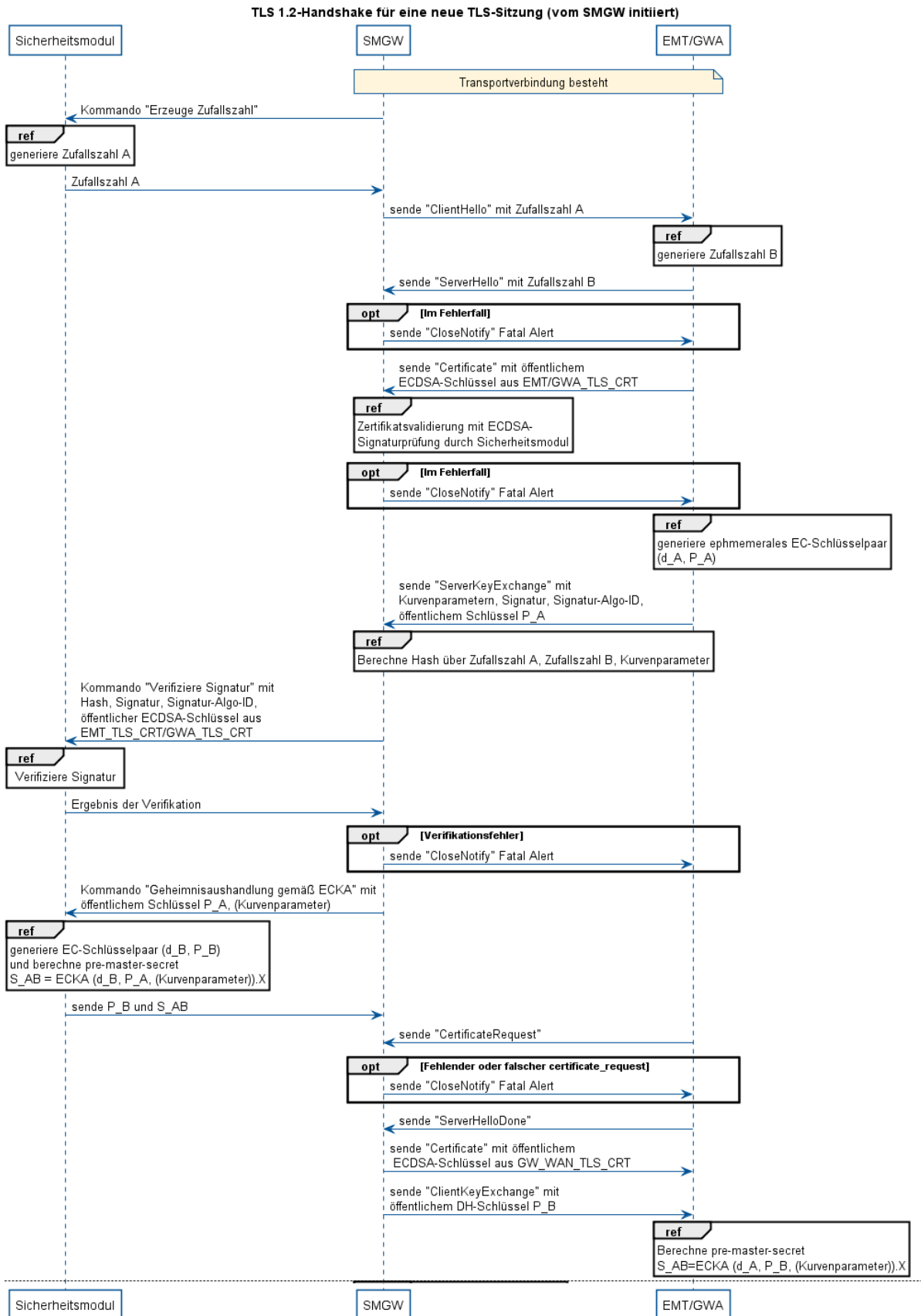


Abbildung 5.1. Interaktion zwischen Gateway und Sicherheitsmodul beim TLS 1.2-Handshake 1/2

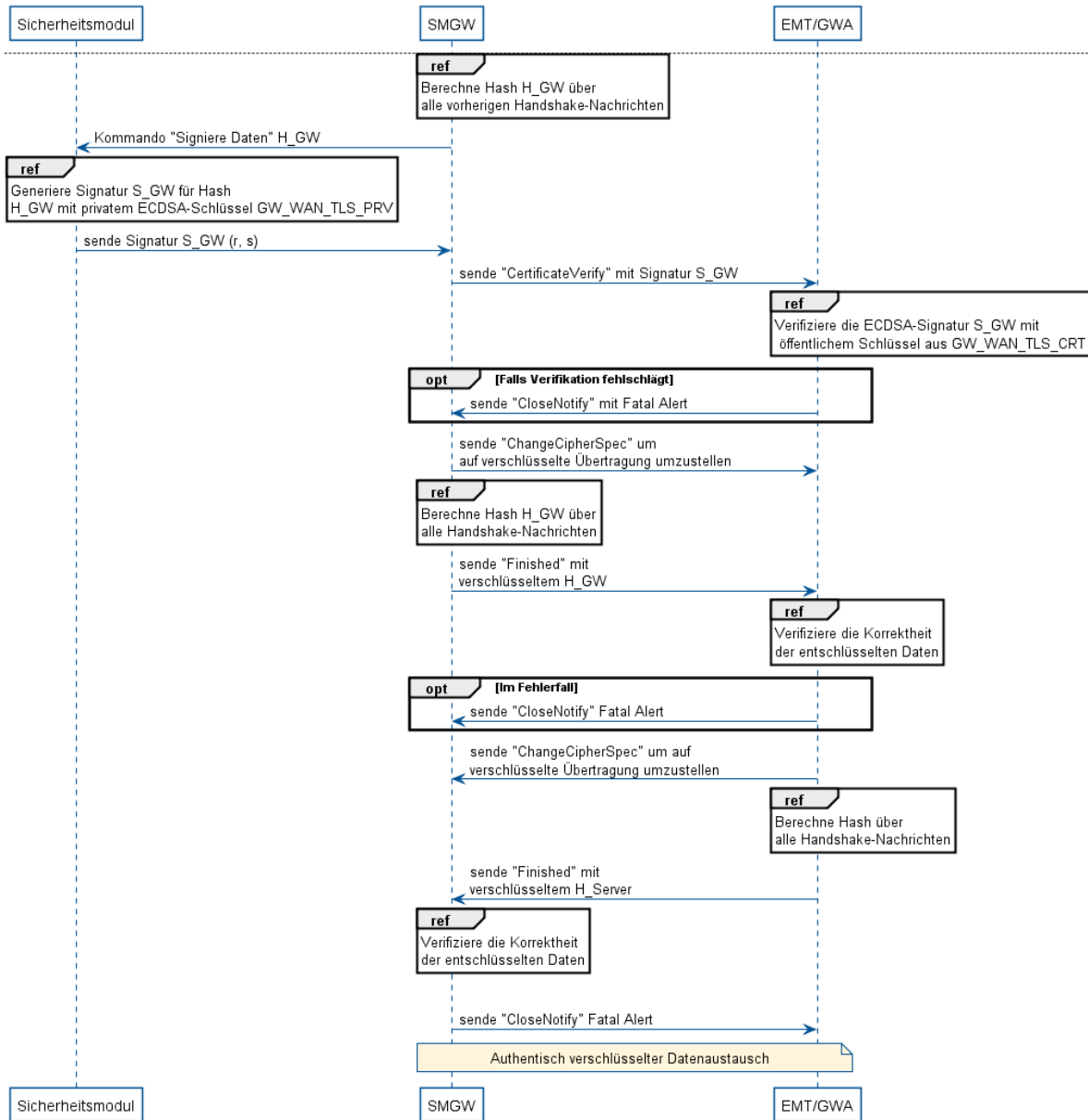


Abbildung 5.2. Interaktion zwischen Gateway und Sicherheitsmodul beim TLS 1.2-Handshake 2/2

Die Reihenfolge der TLS-Kommandos beim TLS-Handshake kann von der in ►Abbildung 5.1 und ►Abbildung 5.2 gezeigten Reihenfolge eventuell abweichen. Die Abbildungen sind diesbezüglich lediglich exemplarisch und informativ zu verstehen. Ausschlaggebend ist die Anforderung in [TR-03109-2], aus der sich Abhängigkeiten bezüglich der Reihenfolge der skizzierten Kommandos ergeben.

5.1.2. Nutzung des Sicherheitsmoduls bei der CMS Inhaltsdatensicherung

Das SMGW **MUSS** zur authentischen Verschlüsselung von Inhaltsdaten-Nachrichten einer WAN-Kommunikation ein hybrides (symmetrisch, asymmetrisches) Verfahren gemäß [TR-03109-3] unterstützen. [REQ.WFA.KryptoImplementierungCms.10]

- Das SMGW **MUSS** das Sicherheitsmodul verwenden, um die Schlüsselaushandlung gemäß Elliptic Curve Diffie-Hellman durchzuführen. [REQ.WFA.KryptoImplementierungCms.20]

- Das SMGW **MUSS** den oder die symmetrischen Schlüssel für die authentische Verschlüsselung der Inhaltsdaten über eine Schlüsselableitungsfunktion (KDF) nach den Vorgaben aus [TR-03109-3] berechnen. [REQ.WFA.KryptoImplementierungCms.30]¹
- Das SMGW **MUSS** das Sicherheitsmodul zur Generierung von Zufallszahlen für symmetrische Verschlüsselung und die Signaturerzeugung verwenden. [REQ.WFA.KryptoImplementierungCms.40]
- Das SMGW **MUSS** das Sicherheitsmodul zur Signaturerzeugung basierend auf elliptischen Kurven verwenden. [REQ.WFA.KryptoImplementierungCms.50]

Das SMGW **MUSS** die kryptographischen Algorithmen und Schlüssellängen gemäß [TR-03109-3] verwenden. [REQ.WFA.KryptoImplementierungCms.60]

►Abbildung 5.3 zeigt exemplarisch für AES im CBC-CMAC-Mode die Interaktion zwischen SMGW und Sicherheitsmodul für die Inhaltsdatenverschlüsselung, Integritätssicherung und Signierung auf. Dabei wird angenommen, dass der öffentliche Schlüssel des Empfängers mit dem dazugehörigen privaten Schlüssel im Besitz des Empfängers auf der WAN-Seite ist.

Die Reihenfolge der Kommandos kann von der in den Abbildungen gezeigten Reihenfolge abweichen. Die Abbildungen sind diesbezüglich lediglich exemplarisch und informativ zu verstehen. Ausschlaggebend ist die Anforderung in [TR-03109-2], aus der sich Abhängigkeiten bezüglich der Reihenfolge der skizzierten Kommandos ergeben.

¹ Für AES-GCM wird ein symmetrischer Schlüssel K benötigt und für AES-CBC-CMAC werden zwei Schlüssel K_{enc} und K_{mac} benötigt.

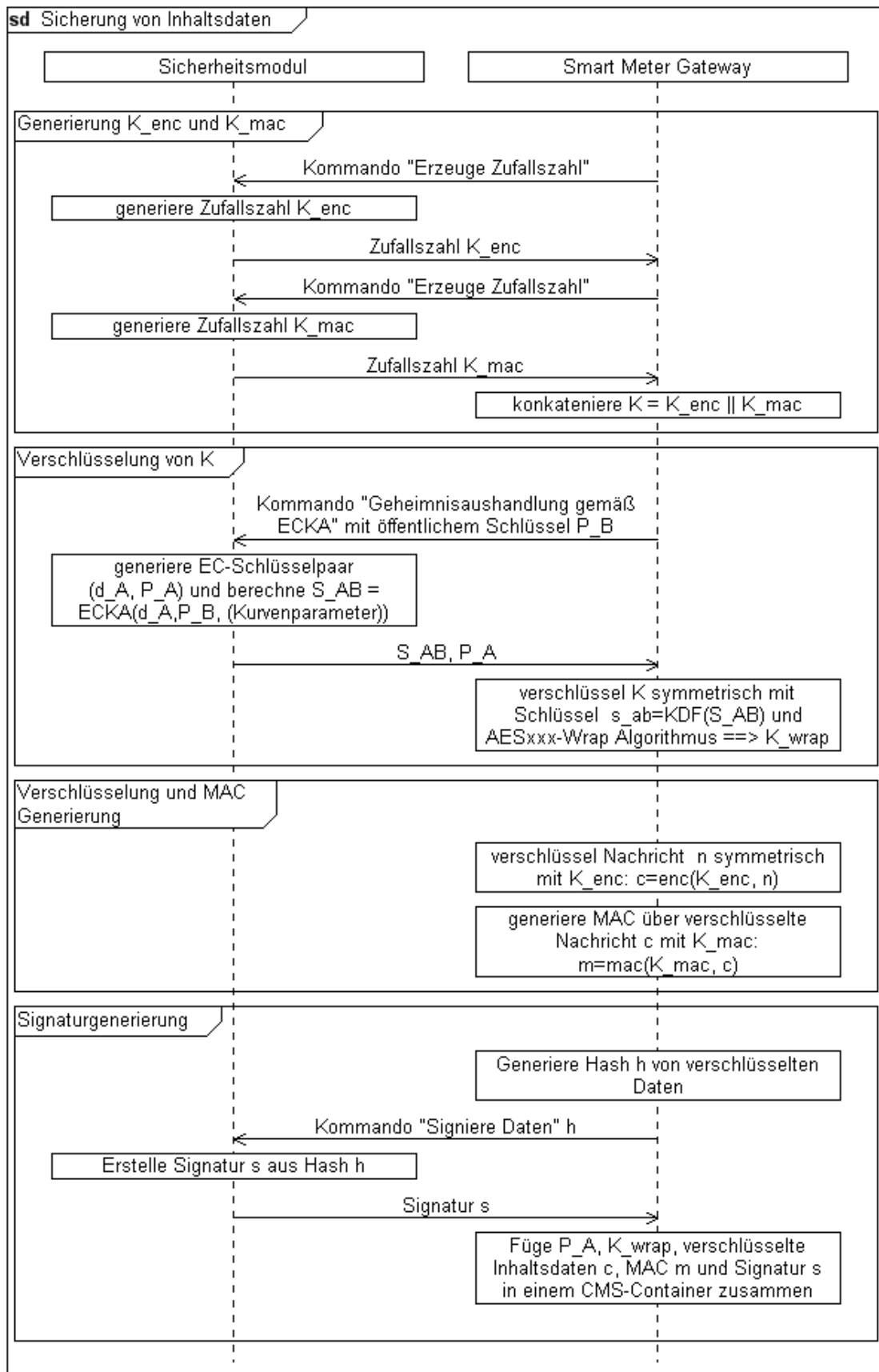


Abbildung 5.3. Interaktion zwischen SMGW und SM bei der Inhaltsdatensicherung mit AES-CBC-CMAC

Der kurzlebige Schlüssel, die verschlüsselte Konkatenation von K_{enc} und K_{mac} , die verschlüsselten Inhaltsdaten c , deren MAC-Prüfsumme m und die Signatur s **MÜSSEN** in einen CMS Container gemäß ▶Abschnitt 3.2.4.2 verpackt werden. [REQ.WFA.KryptoImplementierungCms.70]

5.2. Logdatenformat

Dieses Kapitel beinhaltet Vorgaben an die Syntax von Log-Informationen, die das SMGW an den Schnittstellen (WAN, HAN) zur Verfügung stellen muss.

Gemäß Schutzprofil [PP-0073] werden mindestens drei Klassen von Log-Informationen implementiert. ▶Tabelle 5.1 bietet eine Übersicht über die verschiedenen Logs und die möglichen Zugriffe. Die Anforderungen bezüglich der Zugriffsrechte finden sich in ▶Abschnitt 4.5.

Log-Klasse	Zugriff	Schnittstelle
System-Log	Lesender Zugriff durch den autorisierten GWA.	WAN-Schnittstelle
System-Log	Lesender Zugriff durch den autorisierten Servicetechniker.	HAN-Schnittstelle (IF_GW_SRV)
Anschlussnutzer-Log	Lesender Zugriff nur durch den authentifizierten und autorisierten Anschlussnutzer auf die ihm zugeordneten Log-Einträge.	HAN-Schnittstelle (IF_GW_CON)
Eichtechnisches Log	Lesender Zugriff durch den autorisierten GWA.	WAN-Schnittstelle

Tabelle 5.1 Log-Klassen und erlaubter Zugriff

Die konkrete Implementierung der Log-Informationen kann so realisiert werden, dass tatsächlich drei separate Dateien beschrieben werden. Das SMGW **DARF** System-Log und Anschlussnutzer-Log als Ringspeicher implementieren, sodass bei Überlauf der älteste Log-Eintrag überschrieben wird. [REQ.WFA.Logformat.10] Das SMGW **DARF KEINE** Einträge des Anschlussnutzer-Logs löschen, die vor weniger als 15 Monaten ins Logbuch aufgenommen wurden. [REQ.WFA.Logformat.20] Das SMGW **DARF KEINE** Einträge des Eichtechnischen Logs löschen. [REQ.WFA.Logformat.30]



Anmerkung

Die Größe des Ringspeichers des System-Logs soll entsprechend dimensioniert werden, dass mindestens die Einträge der letzten 15 Monate vorgehalten werden können.

Andere Implementierungen (z.B. als Log-Records in einer Datenbank) sind ebenfalls möglich. Die Zugriffsbeschränkungen auf diese Log-Records müssen allerdings, wie ▶Abschnitt 4.5 beschrieben, auf jeden Fall umgesetzt werden.

▶Tabelle 5.2 enthält Vorschläge zu protokollierender Merkmale für jeden Logeintrag.

Merkmal	Bedeutung
record_number	Eine eindeutige Zahl, die diesen Log-Eintrag kennzeichnet.
datetime	Datum und Uhrzeit in gesetzlicher Zeit, wann der Log-Eintrag geschrieben wurde, mit Differenz zur UTC (Coordinated Universal Time) im Format „±hh:mm“, z.B. „2020-08-14T12:34:47+02:00“.

Merkmal	Bedeutung
level	<p>Log Level zur Einstufung der Wichtigkeit des Logeintrages:</p> <ul style="list-style-type: none"> • „I“: Info Allgemeine Information zum normalen Ablauf. • „W“: Warning Auftreten einer unerwarteten Situation. • „E“: Error Behebbarer Fehler oder Ausnahme, die Bearbeitung wurde alternativ fortgesetzt. • „F“: Fatal Kritischer Fehler, die laufende Bearbeitung wurde abgebrochen. • „X.***“: eXtension Herstellerspezifischer Fehler, Detailangaben folgen dem „X“.
event_type	<p>Art des aufgezeichneten Ereignisses:</p> <ul style="list-style-type: none"> • Auftreten eines sicherheitsrelevanten Ereignisses. • Verbindungsaufbau bzw. -abbau zu WAN-Teilnehmer. • Übertragung abrechnungsrelevanter Messdaten zu WAN-Teilnehmer. • Übertragung nicht abrechnungsrelevanter Messdaten zu WAN-Teilnehmer. • Erstellen/Löschen/Bearbeiten eines Auswertungs-, Zähler- oder Kommunikationsprofils. • Änderung der SMGW Konfiguration durch den GWA. • Änderung eines eichtechnisch zu sichernden Parameters. • Start und Stopp des Log-Mechanismus. • Weitere Ereignisse, die im „Security Target“ eines SMGW Produktes oder in den Security Requirements des Schutzprofils (bzw. in Part 2 der [CC]) definiert sind.
subject_identity	<p>Identität des Subjektes (Prozess, Anwendungskomponente, Benutzer, Profil), durch das ein Ereignis ausgelöst wurde.</p>
outcome	<p>Ergebnis, der mit dem Log-Event verbundenen Aktionen:</p> <ul style="list-style-type: none"> • „S“: Success Die Aktion wurde erfolgreich abgeschlossen • „F“: Failure Die Aktion konnte nicht erfolgreich durchgeführt werden. • „X.***“: eXtension Herstellerspezifisches Ergebnis, Detailangaben folgen dem „X“.
message	<p>Eine das Log-Event zusätzlich beschreibende Erklärung bzw. die Parameter des geloggtten Ereignisses. Diese sind abhängig vom „event_type“.</p>
user_identity	<p>Die Identität des Benutzers, durch den das Ereignis ausgelöst wurde, bzw. für den die Aktion durchgeführt wurde.</p> <p>Falls die Übertragung von Messdaten an WAN-Teilnehmer geloggt wird, muss bei diesen Übertragungen in diesem Feld insbesondere die Identität des Anschlussnutzers geloggt werden, dessen Daten übermittelt wurden.</p> <p>Die Log-Einträge im Anschlussnutzer-Log müssen eindeutig einem Anschlussnutzer zugeordnet werden können. Dazu kann das Attribut „user_identity“ gesetzt werden. Dadurch soll gewährleistet werden, dass verschiedene Anschlussnutzer nur die für sie bestimmten Anschlussnutzer-Log-Einträge in der Anzeigeeinheit dargestellt bekommen (Mandantenfähigkeit des SMGW).</p>

Merkmal	Bedeutung
destination	Adresse des Kommunikationspartners beim Verbindungsaufbau und Datenaustausch (z.B. URL).
evidence	(falls vorhanden) Signatur über den Logeintrag durch das SMGW, zur Beweisbarkeit der Authentizität und des Ursprungs der des Logeintrags.

Tabelle 5.2 Elemente eines Log Eintrages

Die Syntax der Log-Einträge für das System-Log und das Eichtechnische Log beim Auslesen an der WAN-Schnittstelle durch den GWA wird durch entsprechende XML-Datenobjekte gemäß ▶ICS.WFA.Logformat.30 repräsentiert.



ICS.WFA.Logformat.10

Der GHW **MUSS** im ICS angeben, ob das SMGW den ältesten Logeintrag des Anschlussnutzer-Logs bei Überlauf gemäß ▶REQ.WFA.Logformat.10 überschreibt.



ICS.WFA.Logformat.20

Der GHW **MUSS** im ICS angeben, ob das SMGW den ältesten Logeintrag des System-Logs bei Überlauf gemäß ▶REQ.WFA.Logformat.10 überschreibt.



ICS.WFA.Logformat.30

Der GHW **MUSS** im ICS beschreiben, wie die Transfersyntax der Logeinträge von System-Log und Eichlog aufgebaut ist.

5.3. Inhaltliche Daten der Log-Klassen

In diesem Kapitel werden Ereignisse identifiziert, die zwingend zu einem Eintrag in einer der Log-Klassen führen müssen. Weitere Ereignisse können in diesen Log-Klassen protokolliert werden, sofern dadurch die Anforderungen an die Zugriffsberechtigungen, die in ▶Abschnitt 4.5 beschrieben sind, nicht verletzt werden.

5.3.1. Obligatorische Einträge im Eichtechnischen Log

Das Eichtechnische Log dient der Registrierung von Änderungen an eichtechnisch relevanten Soft- und Firmwareanteilen sowie den Konfigurationsprofilen und den zugehörigen Parametern. Des Weiteren müssen im Eichtechnischen Log nach [MessEG]/[MessEV] relevante Ereignisse gespeichert werden, so dass nachträglich erkennbar ist, ob und welche Messwerte verfälscht worden sind.

Alle Informationen und Ereignisse aus ▶Tabelle 5.3 sind im Eichtechnischen Log zu protokollieren. Jeder Log-Eintrag muss dabei den Anforderungen aus ▶Abschnitt 5.2 genügen.

Ereignis / Parameter	Eintrag
Auslösung eines Selbsttests	Das SMGW MUSS jede Initiierung eines Selbsttests gemäß ▶Abschnitt 3.2.9 im Eichtechnischen Log protokollieren. [REQ.WFA.EichlogInhalt.10]
Neuer Zähler	Das SMGW MUSS den Anschluss und die Registrierung eines jeden neuen Zählers im Eichtechnischen Log protokollieren. [REQ.WFA.EichlogInhalt.20]
Entfernung eines Zählers	Das SMGW MUSS das Entfernen eines Zählers vom SMGW im Eichtechnischen Log protokollieren. [REQ.WFA.EichlogInhalt.30]
Änderung von Auswertungsprofilen	Das SMGW MUSS jede Änderung (einschließlich Parametrierung) an Auswertungsprofilen gemäß ▶Abschnitt 4.4.3, die nicht ausschließlich die Parameter "Berechtigungen" oder "Versandzeitpunkte" betreffen, sowie das Einbringen und Löschen von Auswertungsprofilen im Eichtechnischen Log protokollieren. [REQ.WFA.EichlogInhalt.40]

Ereignis / Parameter	Eintrag
Änderung von Zählerprofilen	Das SMGW MUSS jede Änderung (einschließlich Parametrierung) an Zählerprofilen gemäß ▶Abschnitt 4.4.2, sowie das Einbringen und Löschen von Zählerprofilen im Eichtechnischen Log protokollieren. [REQ.WFA.EichlogInhalt.50]
Firmware-Update	Das SMGW MUSS jedes Firmware-Update im Eichtechnischen Log protokollieren. [REQ.WFA.EichlogInhalt.60]
Fehlermeldung eines Zählers	Das SMGW MUSS alle fatalen Fehlermeldungen der angeschlossenen Zähler im Eichtechnischen Log protokollieren. [REQ.WFA.EichlogInhalt.70]
Uhrzeitstellung	Das SMGW MUSS jede Synchronisation der Systemzeit mit dem Zeitserver im Eichtechnischen Log protokollieren. [REQ.WFA.EichlogInhalt.80]
Fehlerfund bei Selbsttest	Das SMGW MUSS jeden bei einem Selbsttest gemäß ▶Abschnitt 3.2.9 festgestellten Fehler im Eichtechnischen Log protokollieren. [REQ.WFA.EichlogInhalt.90]

Tabelle 5.3 Obligatorische Einträge im Eichtechnischen Log

5.3.2. Obligatorische Einträge im Anschlussnutzer-Log

Das Anschlussnutzer-Log dient der Bereitstellung von abrechnungsrelevanten Daten und Tarifinformationen für den Anschlussnutzer, so dass dieser die Möglichkeit erhält nachzuvollziehen, welche Messwerte für die Abrechnung verwendet wurden. Des Weiteren gibt es dem Anschlussnutzer die Möglichkeit zu erfahren, welche Daten an EMT versendet wurden.

Alle identifizierten Informationen und Ereignisse aus ▶Tabelle 5.4 sind im Anschlussnutzer-Log zu protokollieren. Das SMGW **MUSS** Anschlussnutzer-Log-Einträge mit den Informationen aus ▶Abschnitt 5.2 protokollieren. [REQ.WFA.AnLog.10] Das SMGW **MUSS** die Anschlussnutzer-Log-Einträge mindestens für 15 Monate vorhalten. [REQ.WFA.AnLog.20] Das SMGW **DARF** eine längere Vorhaltefrist als 15 Monate für die Anschlussnutzer-Log-Einträge umsetzen. [REQ.WFA.AnLog.30]



Anmerkung

Einige weitere Informationen müssen dem Anschlussnutzer gemäß ▶Abschnitt 3.4.2.1 und ▶Abschnitt 4.5 vom SMGW bereitgestellt werden. Die Art der Bereitstellung wird nicht vorgegeben. Eine Bereitstellung über das Anschlussnutzer-Log ist demnach ebenso zulässig.

Ereignis / Information	Beschreibung
Hinzufügen oder Entfernen von Zählern	Werden neue Zähler dem Anschlussnutzer zugeordnet oder wurden Zähler entfernt oder ausgetauscht, so MUSS das SMGW dies im Anschlussnutzer-Log protokollieren. [REQ.WFA.AnLogInhalt.10]
Versenden von Daten	Das SMGW protokolliert jeden für den Anschlussnutzer relevanten Datenverkehr vom SMGW an EMT und/oder den GWA im Anschlussnutzer-Log, sofern dies durch eine Anforderung dieses Dokuments vorgegeben ist.
Änderung von Auswertungsprofilen	Das SMGW MUSS jede Änderung (einschließlich Parametrierung) der Auswertungsprofile gemäß ▶Abschnitt 4.4.3 im Anschlussnutzer-Log protokollieren. [REQ.WFA.AnLogInhalt.20]
Status des Messsystems	Das SMGW MUSS alle abrechnungsrelevanten Status- und Fehlermeldungen des SMGW sowie der angeschlossenen und dem Anschlussnutzer zugeordneten Zähler im Anschlussnutzer-Log protokollieren. [REQ.WFA.AnLogInhalt.30]
Änderung der Zugangsdaten	Das SMGW MUSS Änderungen der Zugangsdaten des Anschlussnutzers im Anschlussnutzer-Log protokollieren. [REQ.WFA.AnLogInhalt.40]

Tabelle 5.4 Obligatorische Einträge im Anschlussnutzer-Log



Der GWH **MUSS** im ICS angeben, für wie lange das SMGW das Anschlussnutzer-Log gemäß ▶REQ.WFA.AnLog.30 vorhält.

5.3.3. Obligatorische Einträge im System-Log

Das System-Log dient der Bereitstellung von betriebsrelevanten Ereignissen für den GWA bzw. Betreiber des SMGW, sodass dieser die Möglichkeit erhält Störungen, Fehler und weitere Ereignisse im Betrieb nachzuvollziehen.

Mindestens die identifizierten Informationen und Ereignisse aus ▶Tabelle 5.5 sind im System-Log zu protokollieren. Jeder Log-Eintrag muss dabei den Anforderungen aus ▶Abschnitt 5.2 genügen.

Ereignis / Information	Beschreibung
Audit-Daten	Das SMGW MUSS die Audit-Ereignisse für den GWA gemäß [PP-0073] im System-Log protokollieren. [REQ.WFA.SysLogInhalt.10]
Ausfall der Versorgungsspannung	Das SMGW SOLL den Zeitpunkt des Ausfalls der Versorgungsspannung des SMGW im System-Log protokollieren. [REQ.WFA.SysLogInhalt.20]
Wiederkehr der Versorgungsspannung	Das SMGW MUSS nach einem Ausfall der Versorgungsspannung den Zeitpunkt der Wiederkehr der Versorgungsspannung des SMGW im System-Log protokollieren. [REQ.WFA.SysLogInhalt.30]

Tabelle 5.5 Obligatorische Einträge im System-Log



ICS.WFA.SysLogSpannungsausfall.10

Der GWH **MUSS** im ICS angeben, ob das SMGW den Zeitpunkt des Ausfalls der Versorgungsspannung gemäß ▶REQ.WFA.SysLogInhalt.20 protokolliert.

5.4. Eindeutige Geräte-Identifikation des SMGW

Das SMGW **MUSS** eine herstellerübergreifend-eindeutige Identifikationsnummer (*SMGW-ID*) nach [DIN43863-5] mit der Spartenkennzeichnung "Kommunikation" besitzen. [REQ.WFA.SMGW-ID.10]

Das SMGW **MUSS** SM-PKI-Zertifikate besitzen, die auf diese SMGW-ID ausgestellt sind und den Subject Common Name gemäß [SM-PKI-CP] Anhang A enthalten. [REQ.WFA.SMGW-ID.20]

Die resultierende Zeichenfolge enthält nur die Zeichen a-z, 0-9 und Punkt.²

- Identifikationsnummer nach [DIN43863-5]: E BSI0063539421.
- Resultierende kanonische Geräte-ID: ebsi0063539421.sm.

Beispiel 5.1. Kanonischer Gerätebezeichner

Da die Kennung des SMGW aus der Sparte Kommunikation („E“) stammt, beginnt die kanonische Geräte-ID (d.h. der Hostname) eines SMGW immer mit „e“.

² Die Bildungsregel folgt dem DNS Schema: die TR gibt aber keine Verwendung von DNS zur Namensauflösung auf Adressen unterhalb der Ebene von TLS vor. Eine vom GWA verwaltete feste Zuordnung zwischen Hostnamen und Transportadresse im SMGW ist ebenso möglich.

6. Nicht-Funktionale Anforderungen

6.1. Einleitung

Neben den funktionalen Anforderungen an ein Smart Metering System, die in Kapitel ▶2.2 beschrieben wurden, existiert eine Reihe von nicht-funktionalen Anforderungen, die in den folgenden Kapiteln dargestellt werden.

6.2. Versiegelung

Das SMGW schützt sich gegen Angriffe, die einen lokalen Zugriff auf das SMGW voraussetzen. Gemäß [PP-0073] gilt hierbei, dass das unterstellte Angriffspotential in diesem Szenario limitiert ist. Die folgenden Absätze enthalten detaillierte Anforderungen zur Versiegelung des SMGW. Dabei beziehen sich diese Anforderungen ausschließlich auf das Siegel, das im Kontext der Anforderungen dieser TR und der Zertifizierung gemäß [PP-0073] gefordert wird. Technische Anforderungen an eine Versiegelung nach [MessEG]/[MessEV] werden hier nicht thematisiert.



Anmerkung

Je nach Bauart des Gehäuses muss ggf. mehr als ein Siegel verwendet werden. Zur besseren Lesbarkeit wird nachfolgend der Singular (Siegel) verwendet. Die Anforderungen gelten dennoch für alle eingesetzten Siegel.

Das SMGW **MUSS** durch Verwendung eines geeigneten Siegels physische Manipulationen erkennbar machen. Es **DARF NICHT** möglich sein, das Gehäuse des SMGW zu öffnen ohne das Siegel erkennbar zu beschädigen. [REQ.NFA.Siegel.10]

Das Siegel **MUSS** auf dafür geeigneten Siegelflächen angebracht werden, sodass es im normalen Betrieb nicht durch Abnutzung gebrochen wird. [REQ.NFA.Siegel.20]

Ist das Siegel nach Einbau des SMGW nicht mehr sichtbar, so muss der Monteur die Unversehrtheit des Siegels überprüfen und diese durch Anbringen einer zusätzlichen Plombe (bspw. Messstellenbetreiberplombe) an einer über dem SMGW liegenden Abdeckung bestätigen.

Das Gehäuse des SMGW **MUSS** geeignet sein, unbemerkte Manipulationen ohne Bruch des Siegels zu verhindern. Insbesondere **MUSS** das Gehäuse mit Ausnahme der notwendigen Schnittstellen und Lüftungsschlitze vollständig geschlossen sein. Das SMGW **DARF** hierbei **KEINE** Öffnungen besitzen, durch die eine Manipulation möglich ist. [REQ.NFA.Siegel.30]

Das Siegel auf dem Gehäuse des SMGW wird in der gesicherten Produktionsumgebung des Herstellers angebracht. Das Siegel **MUSS** durch den Hersteller angebracht werden. [REQ.NFA.Siegel.40]

SMGW **SOLL** über geeignete Mechanismen das Öffnen des Gehäuses detektieren können und für den Fall der Öffnung geeignet reagieren. Mindestens soll für den Fall einer Gehäuseöffnung der GWA kontaktiert werden. Ferner soll das Ereignis im Eichtechnischen Log und System-Log protokolliert werden. Dieser Mechanismus kann durch mechanische oder magnetische Kontakte, Lichtsensoren, eine Kombination der vorgenannten Mechanismen oder andere, geeignete Mechanismen realisiert werden. [REQ.NFA.Siegel.50]



ICS.NFA.Siegel.10

Der GWH **MUSS** im ICS beschreiben, ob und wie das SMGW eine Öffnung des Gehäuses gemäß ▶REQ.NFA.Siegel.50 detektiert und welche Reaktion vom SMGW ausgeführt wird.

6.3. Einbau des Sicherheitsmoduls

Zur gegenseitigen Authentisierung zwischen SMGW und Sicherheitsmodul **MUSS** das SMGW das PACE-Verfahren verwenden [TR-03109-3]. [REQ.NFA.Einbau.10]

Die dafür benötigte PIN **MUSS** im SMGW geeignet geschützt werden. Der GWH **MUSS** diesen Mechanismus von einer CC-Prüfstelle sicherheitstechnisch begutachten lassen. [REQ.NFA.Einbau.20]

Für das sicherheitstechnische Gutachten **MUSS** die Prüfstelle analog zu der [CEM] nachweisen, dass das vorgeschlagene Verfahren zum Schutz der SMGW PIN resistent ist gegen einen Angreifer mit folgenden Eigenschaften:

- Elapsed Time one month
- Expertise Proficient
- Knowledge of TOE Restricted
- Windows of Opportunity Easy
- Equipment Specialized

[REQ.NFA.Einbau.30]

Literaturverzeichnis

- [CC] *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4*. CCDB/ISO September 2021.
- [CEM] *Common Methodology for Information Technology Security Evaluation*. CCRA. April 2017.
- [DIN43863-5] *E DIN 43863-5:2012-04 (DIN VDE 0418-63-5) - Herstellerübergreifende Identifikationsnummer für Messeinrichtungen*. 2012 . VDE|DKE K461
- [DS] *TR-03109-1 Detailspezifikationen*. Bundesamt für Sicherheit in der Informationstechnik 2021.
- [EN13757-1] *DIN EN 13757-1 - Kommunikationssysteme für Zähler - Teil 1: Datenaustausch*. 2014 . DIN/CEN TC294
- [EN13757-3] *DIN EN 13757-3 - Kommunikationssysteme für Zähler - Teil 3: Anwendungsprotokolle*. 2018 . DIN/CEN TC294
- [EN62056-6-1] *EN 62056-6-1: Electricity metering data exchange - The DLMS/COSEM suite - Part 6-1: Object Identification System (OBIS)*. IEC TC13 2017 .
- [ICSF] *GridWise Interoperability Context-Setting Framework*. GridWise Architecture Council 2008.
- [IEEE 802.3i] *IEEE Std 802.3i-1990 (Clauses 13 and 14), 10 Mb/s UTP MAU, 10 BASE-T*. IEEE.
- [ISO/IEC-Voc] *Standardization and related activities - General vocabulary*. ISO/IEC Guide 2:2004 2004.
- [MessEG] *Gesetz über das Inverkehrbringen und die Bereitstellung von Messgeräten auf dem Markt, ihre Verwendung und Eichung sowie über Fertigpackungen (Mess- und Eichgesetz - MessEG)*. Bundesministerium für Wirtschaft und Energie.
- [MessEV] *Verordnung über das Inverkehrbringen und die Bereitstellung von Messgeräten auf dem Markt sowie über ihre Verwendung und Eichung (Mess- und Eichverordnung - MessEV)*. Bundesministerium für Wirtschaft und Energie.
- [MsbG] *Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz - MsbG)*. Bundesministerium für Wirtschaft und Energie.
- [OMSS4] *Open Metering System Specification - Volume 2 Primary Communication - Issue 4.3.3*. 2020 . OMS-Group
- [PP-0073] *BSI-CC-PP-0073-2014, v1.3.1 Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP)*. 2021 . Bundesamt für Sicherheit in der Informationstechnik
- [PP-0077] *BSI-CC-PP-0077-2014, v1.3 Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP)*. 2014 . Bundesamt für Sicherheit in der Informationstechnik
- [RFC2119] *Key words for use in RFCs to Indicate Requirement Levels*. IETF und Scott Bradner . 1997 .
- [RFC3274] *Compressed Data Content Type for Cryptographic Message Syntax (CMS)*. IETF und P. Gutmann . 2002 .
- [RFC3986] *Uniform Resource Identifier (URI): Generic Syntax*. IETF, Tim Berners-Lee , Roy T. Fielding und Larry Masinter . 2005 .
- [RFC5083] *Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type*. IETF und R. Housley . 2007 .

- [RFC5280] *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. IETF, D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley und W. Polk. 2008.
- [RFC5480] *Elliptic Curve Cryptography Subject Public Key Information*. IETF, Turner, Brown, Yiu, Housley und Polk. 2009.
- [RFC5639] *Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation*. IETF, Lochter und Merkle. 2010.
- [RFC5652] *Cryptographic Message Syntax (CMS)*. IETF und R. Housley. 2009.
- [RFC5905] *Network Time Protocol Version 4: Protocol and Algorithms Specification*. IETF, D. Mills, J. Martin, J. Burbank und W. Kasch. 2010.
- [RFC7230] *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*. IETF, R. Fielding und J. Reschke. 2014.
- [SM-PKI-CP] *SM-PKI-CP - Certificate Policy für die SM-PKI v1.1.1*. 2017. Bundesamt für Sicherheit in der Informationstechnik
- [TR-02102-1] *BSI TR-02102-1: Kryptographische Verfahren und Schlüssellängen*. Jährlich aktualisiert. Bundesamt für Sicherheit in der Informationstechnik
- [TR-03109-1-I] *Technische Richtlinie BSI-TR-03109-1, Anlage I: CMS-Datenformat für die Inhaltsdatenverschlüsselung und -signatur, v1.0.9*. 2019. Bundesamt für Sicherheit in der Informationstechnik
- [TR-03109-1-VI] *Technische Richtlinie BSI-TR-03109-1, Anlage VI: Betriebsprozesse, v1.0*. 2013. Bundesamt für Sicherheit in der Informationstechnik
- [TR-03109-1-VIII] Bundesamt für Sicherheit in der Informationstechnik *Technische Richtlinie BSI-TR-03109-1, v1.1, Anlage VIII: Lebenszyklus*. 2021.
- [TR-03109-2] *Technische Richtlinie BSI-TR-03109-2: Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls*. 2014. Bundesamt für Sicherheit in der Informationstechnik
- [TR-03109-3] *Technische Richtlinie BSI-TR-03109-3: Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen*. 2014. Bundesamt für Sicherheit in der Informationstechnik
- [TR-03109-4] *Technische Richtlinie BSI-TR-03109-4: Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways*. 2014. Bundesamt für Sicherheit in der Informationstechnik
- [TR-03109-6] *Technische Richtlinie BSI TR-03109-6: Smart Meter Gateway Administration*. 2015. Bundesamt für Sicherheit in der Informationstechnik
- [TR-03111] *Technische Richtlinie BSI-TR-03111 v2.10 Elliptic Curve Cryptography*. 2018. Bundesamt für Sicherheit in der Informationstechnik
- [TR-03116-3] *BSI TR-03116-3: Kryptographische Vorgaben für Projekte der Bundesregierung Teil 3 - Intelligente Messsysteme*. Jährlich aktualisiert. Bundesamt für Sicherheit in der Informationstechnik
- [TR50572] *Functional reference architecture for communications in smart metering systems*. CEC/CLC/ETSI 2011.
- [VDE0418-63-8] *DIN VDE V 0418-63-8 (Bisher E DIN43863-8): Smart Meter Gateway – Klassen-Definition zur TR 03109 nach COSEM*. VDE|DKE K461 2021.
- [VDE0418-63-9] *DIN VDE 0418-63-9 (Bisher DIN43863-9): Elektrizitätszähler – Teil 9: Intelligentes Kommunikationsprotokoll für Stromzähler (SML)*. VDE|DKE K461 2018.
- [X.690] *ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*. 07/2002. ITU
- [XML1.0] World Wide Web Consortium. *Extensible Markup Language (XML) 1.0 (Fifth Edition)*. 2008.

Glossar

Abgeleitete Register	Container, in dem das SMGW Stoff- oder Energiemengen kumuliert.
Abgeleitete Werteliste	Container zur Aufnahme einer Liste von Datensätzen. Im Kontext der traditionell benutzten Formulierung entsprechen diese Container den „Lastgängen / Zählerstandsgängen“. Abgeleitete Wertelisten können auch <i>originäre Messwerte</i> beinhalten.
Abrechnungsrelevanter Messwert	Ein mit einem geeichten und zertifizierten SMGW empfangener bzw. berechneter, gültiger und zeitgestempelter Zahlenwert einer <i>Messgröße</i> zuzüglich seiner Einheit zur Verwendung für die Abrechnung im geschäftlichen Verkehr.
Abrechnungstechnischer Kalendertag	Kalendertag, der für Abrechnungszwecke bei Elektrizität um 0:00h und bei Gas um 6:00h beginnt.
Abrechnungszeitraum	Zeitraum, für den eine Abrechnung erstellt wird.
Aggregation	Funktion im SMGW, die Momentanwerte aus einem Zeitraum zu aggregierten Werten zusammenfasst. Bildungsregeln definieren, welche <i>aggregierten Werte</i> gebildet werden sollen.
Aggregationsperiode	Eine Aggregationsperiode bestimmt, über welche Zeiträume Momentanwerte jeweils aggregiert werden sollen.
Aggregierte Werte	Auf Basis von Momentanwerten erzeugte Werte (z.B. Minimum-, Maximum-, oder Mittelwerte).
Aktueller Wert	Als aktueller Wert wird der letzte, von einem Zähler übermittelte und im SMGW registrierte Messwert bezeichnet.
Anschlussnutzer	Technischer Akteur am SMGW, der elektrische Energie, thermische Energie, Gas oder Wasser bezieht oder erzeugt und zur Nutzung des Netzanschlusses berechtigt ist. Der Anschlussnutzer verwendet zur Interaktion mit dem SMGW ein Kommunikationsgerät (z.B. Display). Der Technische Akteur Anschlussnutzer ist beispielsweise ein Letztverbraucher oder Anlagenbetreiber gemäß [MsbG]. In früheren Versionen dieses Dokuments wurde und in referenzierten Dokumenten wird der Anschlussnutzer auch als Letztverbraucher bezeichnet. Gleiches gilt für Kompositionen wie dem Letztverbraucher-Log.
Anschlussnutzerkennung	Der im SMGW eindeutige Bezeichner für einen Anschlussnutzer.
Auswertungsprofil	Ein Auswertungsprofil parametrisiert ein <i>Regelwerk</i> , für einen konkreten Anwendungsfall.
Bilanzierung	Bilanzkreisabrechnung gemäß Marktkommunikation.
Eichtechnisches Log	Logbuch, in dem die nach [MessEG]/[MessEV] relevanten Ereignisse (z.B. erkannte Verfälschungen von Messungen, fehlgeschlagene Zeitsynchronisierungen) aufgezeichnet werden. Außerdem erfolgt hier die Registrierung von

	Änderungen an eichtechnisch relevanten Parametern (z.B. das Stellen der Geräteuhr). Dieses Log kann nur von dem autorisierten GWA eingesehen werden und wird bei Bedarf vom GWA den Eichbehörden zur Verfügung gestellt.
Einspeisung	Von einer Erzeugungs- oder Speicheranlage in ein Energienetz eingespeiste <i>Energiemenge</i> .
Stoff- oder Energiemenge	Menge an Elektrizität oder Gas, soweit sie zur leitungsgebundenen Energieversorgung und Energieeinspeisung verwendet werden. Bei Gas bezeichnet der Begriff das Gasvolumen.
Energievorschub	Positive Differenz $Z_2 - Z_1$ zwischen zwei Zählerständen Z_1, Z_2 . Wobei Z_2 nach Z_1 gemessen wurde.
Erzeugungsanlage	Anlage zur Erzeugung von Elektrizität, die an das Elektrizitätsversorgungsnetz angeschlossen ist oder für Gas.
Geräte-ID	Der eindeutige Bezeichner eines Gerätes.
Geräte-ID des Zählers	Der eindeutige Bezeichner des Zählers an dem der Anschlussnutzer den Zähler eindeutig identifizieren kann.
Gültigkeitszeitraum	Der Zeitraum für den ein <i>Regelwerk</i> mit gleichbleibenden Parametern im SMGW arbeiten muss. Der Zeitraum kann im Fall einer Tarifabbildung an die Vertragslaufzeiten des <i>Tarifs</i> geknüpft sein.
HAN-Kommunikationsprofil	HAN-Kommunikationsprofile legen die Parameter für die Kommunikation des SMGW zu Anschlussnutzern oder Servicetechnikern fest.
kanonisierte Form	Zur Verarbeitung und zum Vergleich normalisierte Darstellung mit fester Länge, ohne Leerzeichen.
Kommunikationsprofil	Ein Oberbegriff für alle anderen Profile zur Festlegung von Parametern für die Kommunikation. Siehe <i>HAN-Kommunikationsprofil</i> , <i>WAN-Kommunikationsprofil</i> und <i>Proxy-Kommunikationsprofil</i> . Ein Kommunikationsprofil kann durch eine oder mehrere Datenstrukturen realisiert werden.
Kommunikationsszenario	Beschreibt die Komposition des Protokollstapels und die Datenflussrichtungen an einer Schnittstelle zwischen SMGW und einem weiteren Akteur.
Konfigurationsprofile	Oberbegriff für <i>Auswertungsprofile</i> , <i>Kommunikationsprofile</i> und <i>Zählerprofile</i> . Konfigurationsprofile entsprechen der semantischen Beschreibung von zusammenhängenden Parametern.
Messeinrichtung	Siehe Zähler .
Messgröße	Physikalische Größe, deren Wert durch eine Messung bestimmt wird (z.B. Wirkleistung, Blindleistung, Spannung, Volumen).
Messart	Art, auf die eine Messwert bestimmt wird (z.B. Zeitintegral total, Zeitintegral über eine Periode, Momentanwert, Maximumwert).
Messlokation	Lokation, an der Energie gemessen wird und die alle technischen Einrichtungen beinhaltet, die zur Ermittlung und ggf. Übermittlung der Messwerte erforderlich sind. Zusatzinformation: In einer Messlokation wird jede relevante

	physikalische Größe zu einem Zeitpunkt maximal einmal ermittelt. Messlokationen werden mittels Zählpunktbezeichnungen eindeutig identifiziert.
Messwert	Ein mit einem <i>Zähler</i> gemessener Zahlenwert einer <i>Messgröße</i> zuzüglich seiner Einheit.
Messwertliste	Eine Messwertliste enthält alle Messwerte eines Zählers, die für Messwertverarbeitungen in einem <i>Regelwerk</i> verwendet werden. Zusätzlich zum <i>Messwert</i> wird der Zeitstempel und die <i>Statusinformation</i> des Messwerts hinterlegt. In der technischen Umsetzung kann die Messwertliste über eine <i>abgeleitete Werteliste</i> modelliert werden.
Netzzustandsdaten	Netzzustandsdaten sind nicht <i>abrechnungsrelevante Messwerte</i> , die für Betriebsführungszwecke benötigt werden (z.B. Spannung, Phasenwinkel, Frequenz) und die nicht für <i>Tarifierung</i> oder <i>Bilanzierung</i> verwendet werden.
Neue Messgröße	Vom SMGW aus physikalischen Messgrößen berechnete <i>Messgröße</i> . <i>Messwerte</i> neuer Messgrößen werden in abgeleiteten Registern abgelegt.
OBIS-Kennzahl	Identifikation von Messwerten oder anderer abstrakter Daten.
Originärer Wert	Ein mit einem Messgerät gemessener Zahlenwert einer <i>Messgröße</i> zuzüglich seiner Einheit.
Proxy-Kommunikationsprofil	Ein Proxy-Kommunikationsprofil ist ein spezielles Kommunikationsprofil für die HAN Schnittstelle. Proxy-Kommunikationsprofile legen Parameter für die Kommunikation zu CLS im HAN und EMT im WAN fest.
Pseudonymisierung	Bei der Pseudonymisierung im SMGW wird für den Versand von <i>Messwerten</i> die mit zu sendende <i>Geräte-ID des jeweiligen Zählers</i> durch ein Pseudonym ersetzt, um die Identifizierung des Zählers und damit des Anschlussnutzers zu erschweren. Das verwendete Pseudonym wird jeweils vom GWA vorgegeben.
Regelwerk	Die Vorschrift zur Verknüpfung von Eingangsgrößen, Bedingungen und Berechnungen zur Umschaltung von Tarifen. Ein Regelwerk besteht aus mehreren Regeln, die auch abgeleitete Werte desselben Regelwerks verwenden können. Regelwerke werden vom <i>Auswertungsprofil</i> parametrieren.
Register	Siehe <i>Abgeleitete Register</i> .
Registrierperiode	Eine Registrierperiode ist der Zeitraum zur Ermittlung eines Energiemesswertes für einen <i>Zählerstandsgang</i> .
Sollregistrierzeitpunkt	Zeitpunkt mit Datum und sekundengenauer Uhrzeit, dessen Uhrzeit ein Vielfaches einer <i>Registrierperiode</i> ab der Tageszeit 00:00:00 Uhr bei Elektrizität darstellt. Für eine <i>Registrierperiode</i> der Länge 15 Minuten bei Elektrizität: 00:15:00, 00:30:00, 00:45:00, ..., 00:00:00 des Folgetages. <i>Originäre Messwerte</i> werden im SMGW der jeweils gültigen Registrierperiode zugeordnet. Die Sollregistrierzeitpunkte bilden die Zeitbasis der abgeleiteten Werteliste .
Statusinformation	Zusätzliche Information zu einem <i>Messwert</i> .
Tarif	Siehe <i>Tarifierung</i> .
Tarifierung	Die Tarifierung ist ein Aufteilen der gemessenen elektrischen Energie bzw. Volumenmengen gemäß den hinterlegten <i>Auswertungsprofilen</i> in verschiedene <i>Tarifstufen</i> .

Tarifstufe	Eine Tarifstufe bezieht sich auf den Anteil einer <i>Stoff- oder Energiemenge</i> , die mit einem eigenen Preis abgerechnet werden soll. Tarifstufen werden den <i>abgeleiteten Register</i> zugeordnet.
Tarifumschaltzeitpunkt	Zeitpunkt zu dem in eine bestimmte <i>Tarifstufe</i> geschaltet werden soll. Diese werden in <i>Auswertungsprofilen</i> parametrisiert. Ein solcher Zeitpunkt fällt immer auf einen <i>Sollregistrierzeitpunkt</i> .
Tarifwechselliste	Liste von <i>Tarifwechselzeitpunkten</i> .
Tarifwechselzeitpunkt	Zeitpunkt zu dem in eine bestimmte <i>Tarifstufe</i> geschaltet worden ist. Hier sind die tatsächlichen aufgetretenen Ist-Zeitpunkte gemeint.
Transparenter Kanal	Ein vom SMGW bereitgestellter Kommunikationskanal zwischen einem CLS im HAN und einem EMT im WAN. Dabei leitet das SMGW die eintreffenden Informationen zwischen CLS und EMT unverändert weiter.
Verbrauch	Von einem Anschlussnutzer verbrauchte <i>Stoff- oder Energiemenge</i> .
WAN-Kommunikationsprofil	Ein Kommunikationsprofil legt die Parameter für die Kommunikation zu einem autorisierten EMT im WAN oder dem GWA fest.
Zähler	Messgerät, das allein oder in Verbindung mit anderen Messeinrichtungen für die Ermittlung eines oder mehrerer <i>Messwerte</i> eingesetzt wird.
Zählerprofil	Ein Zählerprofil beschreibt die Konfiguration für das SMGW, die notwendig ist, um mit einem <i>Zähler</i> zu kommunizieren und die aktuellen <i>Messwerte</i> zu erfassen.
Zählerstand	Der Zählerstand ist ein <i>Messwert</i> eines <i>Zählers</i> . Gemessen wird die <i>Stoff- oder Energiemenge</i> die bis zum jeweiligen Ableszeitpunkt verbraucht oder eingespeist wurde.
Zählerstandsgang	Die Messung einer Reihe viertelstündig ermittelter Zählerstände von elektrischer Arbeit und stündlich ermittelter Zählerstände von Gasmengen.
Zeitbedingung	Zeitraum $[t_1, t_2)$ bestehend aus zwei <i>Tarifumschaltzeitpunkten</i> t_1 und t_2 . Eine Zeitbedingung ist solange erfüllt wie für die aktuelle Zeit t gilt $t_1 \leq t < t_2$.

Datenobjekte

In diesem Teil des Glossars finden sich die von den FA verwendeten Datenobjekte.

SMGW-ID	Identifiziert das SMGW eindeutig in der SM-PKI und entspricht dem Namen des Inhabers der SMGW-Zertifikate (GW_WAN_SIG_CERT, GW_WAN_ENC_CERT, GW_WAN_TLS_CERT). Die "SMGW-ID" wird nach [SM-PKI-CP] Anhang A für das SMGW basierend auf der <i>kanonisierten Form</i> der herstellerübergreifend eindeutigen Messgeräteidentifikation nach [DIN43863-5] Kapitel 3 gebildet.
GW_HAN_TLS_CERT	Das TLS-Authentifizierungszertifikat des SMGW an der HAN-Schnittstelle (s. Detailspezifikation ☞ Zertifikatsprofile am HAN) basierend auf [RFC5280] Kapitel 4.
SRV_HAN_TLS_CERT	Das TLS-Authentifizierungszertifikat des Servicetechnikers als HAN-Teilnehmer (s. Detailspezifikation ☞ Zertifikatsprofile am HAN) mit dem basierend auf [RFC5280] Kapitel 4

CON_HAN_TLS_CERT	Das TLS-Authentifizierungszertifikat des Anschlussnutzers (Consumer) als HAN-Teilnehmer (s. Detailspezifikation ↗ Zertifikatsprofile am HAN) basierend auf [RFC5280] Kapitel 4
CLS_HAN_TLS_CERT	Das TLS-Authentifizierungszertifikat eines CLS-Gerätes als HAN-Teilnehmer (s. Detailspezifikation ↗ Zertifikatsprofile am HAN) mit dem basierend auf [RFC5280] Kapitel 4
GWACA_SIG_CERT	Das Signaturzertifikat der CA des GWA, die die Zertifikate der Servicetechniker für Diagnose an der HAN-Schnittstelle des SMGW ausstellt (s. Detailspezifikation ↗ Zertifikatsprofile am HAN). Das Zertifikat hat die Eigenschaften eines X.509 basierend auf [RFC5280] Kapitel 4
GWHCA_SIG_CERT	Das Signaturzertifikat der CA des GWH, die die Zertifikate der Servicetechniker für Diagnose an der HAN-Schnittstelle des SMGW ausstellt (s. Detailspezifikation ↗ Zertifikatsprofile am HAN). Das Zertifikat hat die Eigenschaften eines X.509 basierend auf [RFC5280] Kapitel 4

Anhang A. Abkürzungsverzeichnis

Abkürzung	Beschreibung
aEMT	Aktiver Externer Marktteilnehmer
AFL	Authentication and Fragmentation Layer, Wireless MBUS
API	Application Programming Interface
APL	Application Protocol Layer, Wireless MBUS
ARP	Address Resolution Protocol
ASN	Abstract Syntax Notation
BER	Basic Encoding Rules (ASN.1)
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CLS	Controllable Local System
CMS	Cryptographic Message Syntax, Inhaltsdatensicherung nach ASN.1
CON	Consumer bzw. Anschlussnutzer
COSEM	COmpanion Specification for Energy Metering
DER	Distinguished Encoding Rules (ASN.1)
DS	Detailspezifikation
EMT	Externer Marktteilnehmer
EnWG	Energiewirtschaftsgesetz
GDEW	Gesetz zur Digitalisierung der Energiewende
GWA	Smart-Meter-Gateway-Administrator
GWH	Smart-Meter-Gateway-Hersteller
HAN	Home Area Network
HDLC	High Level Data Link Control
HKS	HAN-Kommunikationsszenario
HTTP	HyperText Transfer Protocol
IC	Interface Class (für COSEM)
ICS	Implementation Conformance Statement
IETF	Internet Engineering Task Force
IP	Internet Protocol
KS	Kommunikationsszenario
LKS	LMN-Kommunikationsszenario
LMN	Local Meter Network
wM-Bus	Wireless Meter Bus
MessEG	Mess- und Eichgesetz

Abkürzung	Beschreibung
MessEV	Mess- und Eichverordnung
MK	Master Key
MSB	Messstellenbetreiber
MsbG	Messstellenbetriebsgesetz
MTR	Messeinrichtung
N/A	Nicht anwendbar
NTP	Network Time Protocol
OBIS	OBject Identification System (für COSEM)
PSK	Pre-Shared Key, zuvor vereinbarter symmetrischer Schlüssel
PTB	Physikalisch-Technische Bundesanstalt
RFC	Request For Comments
RTT	Round Trip Time
SM	Sicherheitsmodul
SM-PKI	Smart-Meter - Public Key Infrastructure
SMGW	Smart-Meter-Gateway
SML	Smart Message Language
SNI	Server Name Indication
SRV	Servicetechniker des SMGW
TCP	Transmission Control Procotol
TLS	Transport Layer Security, Transportsicherungsprotokoll
TPL	Transport Protocol Layer, Wireless MBUS
TR	Technische Richtlinie
UDP	User Datagram Protocol
UTC	Coordinated Universal Time, Zeitskala
WAN	Wide Area Network
WKS	WAN-Kommunikationsszenario
XML	Extendable Markup Language

Tabelle A.1 In der TR verwendete Abkürzungen

Anhang B. Changelog

Kapitel	Abschnitt	Änderungen
Global	-	<ul style="list-style-type: none"> • Letztverbraucher in Anschlussnutzer umbenannt • Anlage VII aufgelöst und Anforderungen der Profile BASIS und NETZ in die Stammrichtlinie überführt • Vergabe von Anforderungs-IDs für normative und optionale Anforderungen • Informative Anlage VIII für den Lebenszyklus des SMGW ergänzt
Kapitel 1	-	<ul style="list-style-type: none"> • Grundlegende Aktualisierung • Definition ICS und Requirements • Aufnahme Nachweispflicht zur Interoperabilität
Kapitel 2	-	<ul style="list-style-type: none"> • Aktiver EMT als Technische Rolle eingeführt • Interoperabilitätsmodell aus bisheriger Anlage VII ergänzt
Kapitel 3	Abschnitt 3.2	<ul style="list-style-type: none"> • WAF4: entfällt, da er Bestandteil des WAF2 ist • WKS für WAKEUP und TLSPROXY benannt • Abschnitt Pseudonymisierung nach Abschnitt 4.3 verschoben • Sicherung der Kommunikationsverbindungen ergänzt • WAN-Kommunikationsprofile ergänzt • WAN-Kommunikationsprotokolle ergänzt • Anforderungen an die Zeitführung, die nicht NTP-spezifisch sind, ergänzt • Neue Funktion: optionalen Netzwerkdiagnoseservice ergänzt • Anforderungen an Selbsttests des SMGW ergänzt
	Abschnitt 3.3	<ul style="list-style-type: none"> • LKS1: Konkretisiert auf bidirektionale, drahtgebundene Kommunikation mit Absicherung durch TLS, SML, HDLC • LKS2: Konkretisiert auf unidirektionale, drahtlose Kommunikation mit Absicherung durch symmetrische Kryptografie und Applikationsprotokoll wireless M-BUS
	Abschnitt 3.4	<ul style="list-style-type: none"> • HAF1: Datenbereitstellung historischer Werte für Letztverbraucher basierend auf Registrierperioden-bezogenen Zählerstandsgängen und Tageswerten • Neue Funktion: HAF4, Herstellen der GWA-Kommunikation durch den Servicetechniker ergänzt • Neue Funktion: HAF5, Auslösen von Selbsttest-Funktionen durch den Servicetechniker ergänzt • Neue Funktion: Optionales Steuerungsprotokoll TLS-SNI ergänzt • Optionale zweite physische HAN-Schnittstelle ergänzt • Neue Funktion: Optionale automatische Adresskonfiguration für HAN-Teilnehmer ergänzt

Kapitel	Abschnitt	Änderungen
Kapitel 4	-	<ul style="list-style-type: none"> Integration der Errata-Dokumente zu TAF 2, 9, 10, 14 TAF 1, 2, 6, 7, 9, 10, 14 nun normativ Optionale TAF entfernt, werden künftig mit der Branche nach Bedarf spezifiziert Kategorisierung der TAF innerhalb verschiedener Abschnitte entfallen Übersicht aller TAF in Abschnitt 4.1 integriert
Kapitel 5	-	<ul style="list-style-type: none"> Weitere obligatorische Einträge ergänzt Eindeutige Geräteidentifikation des SMGW aus bisherigem Abschnitt 3.2.4 verschoben
Literaturverzeichnis	-	Referenzen aktualisiert
DS Kapitel 2	-	Detaillierung des bisherigen Anhang A (Wake-Up-Datenstruktur)
DS Kapitel 3	-	Detaillierung des bisherigen Anhang B (LMN-Zertifikate)
DS Kapitel 4	-	Detaillierung des bisherigen Anhang C (HAN-Zertifikate)
DS Kapitel 5	-	Verweis auf Anlage I CMS, die künftig in dieses Kapitel integriert wird
DS Kapitel 6	-	RESTful Webservice Protokoll (ersetzt bisherige Anlage II)
DS Kapitel 7	-	Protokoll zur (HAN-)Authentifizierung des Letztverbrauchers mittels Kennung und Passwort (Digest-Authentifizierung)
DS Kapitel 8	-	Verweis auf Protokolle für die bidirektionale LMN-Kommunikation mittels TLS, HDLC (ersetzt bisherige Anlage IVa) gemäß TLS1.2, VDE0418-63-7
DS Kapitel 9	-	<ul style="list-style-type: none"> Protokolle für die Unidirektionale LMN-Kommunikation mittels Wireless M-Bus (ersetzt bisherige Anlagen IIIa und IIIb) mit Crypto-Mode 7 gemäß EN13757-7, EN13757-4, EN13757-3 Neue Funktion: Optionale Übermittlung von Messwertbündeln mit EN13757-3 Compact Profile
DS Kapitel 10	-	Verwendung von SOCKSv5 mit TLS für die Signalisierung im HKS3 (bisher in Abschnitt 3.4.3.3)
DS Kapitel 11	-	Neue Funktion: Verwendung von TLS-ServerNameIndication für die Signalisierung im HKS3
DS Kapitel 12	-	Neue Funktion: Automatische Adresskonfiguration mit mDNS am HAN
DS Kapitel 13	-	Neue Funktion: Netzwerkdiagnoseservice

Tabelle B.1 Changelog von Version 1.1 zu Version 1.0.1

