Bundesamt
für Sicherheit in der
Informationstechnik

Technische Richtlinie BSI TR-03109-1

Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems

Version 1.0, Datum 18.03.2013

Bundesamt für Sicherheit in der Informationstechnik

Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-100

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

Inhaltsverzeichnis

Anlagen

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Zielsetzung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat diese Technische Richtlinie (TR) mit dem Ziel erstellt, Anforderungen an die Funktionalität, Interoperabilität und Informationssicherheit, die eine Kommunikationseinheit eines intelligenten Messsystems erfüllen muss, zu beschreiben.

Die Technische Richtlinie referenziert und ergänzt das Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems [GW_PP], indem die funktionalen Sicherheitsanforderungen an diese Komponente und ihre Einsatzumgebung u.a. um Vorgaben an Kommunikationsprotokolle, Tarif- und Auswertungsprofile und kryptographische Verfahren erweitert werden.

1.2 Zielgruppe

Die Technische Richtlinie richtet sich in erster Linie an Hersteller von Kommunikationseinheiten intelligenter Messsysteme ("Smart Meter Gateways"). Die Konformität eines Produktes zu den Anforderungen dieser TR wird durch eine Prüfung bei einer für dieses Prüfgebiet vom BSI anerkannten Prüfstelle bescheinigt und durch ein Zertifikat des BSI abschließend bestätigt.

1.3 Anwendungsbereich

Die Technische Richtlinie betrachtet Smart Meter Gateways und deren Schnittstellen zu den Kommunikationspartnern, die im Kontext des Smart Metering erforderlich sind.

1.4 Fachlich zuständige Stelle

Fachlich zuständig für die Fortentwicklung des Dokumentes „Technische Richtlinie BSI TR-03109-1: Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems“ ist das Bundesamt für Sicherheit in der Informationstechnik.

Anschrift: Bundesamt für Sicherheit in der Informationstechnik
Abteilung S
Postfach 20 03 63
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.

1.5 Terminologie

Für die genauere Unterscheidung zwischen normativen und informativen Inhalten werden die dem [RFC2119] entsprechenden in Großbuchstaben geschriebenen, deutschen Schlüsselworte verwendet:

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

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

1.6 Aufbau der Technischen Richtlinie

Beginnend mit Kapitel 2 „Technische Einleitung“ wird in einer kurzen Einführung dargelegt, wie die Einbettung des Smart Meter Gateways (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 Smart Meter Gateways“ 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 Rechtemanagement zum Zugriff auf die Messwerte im SMGW festgelegt wird.

In Kapitel 5 „Weitere Funktionale Anforderungen“ werden Anforderungen an das SMGW spezifiziert (z.B. das Logdatenformat, etc.) die neben den in Kapitel 4 dargestellten Funktionen wichtig sind.

Nicht-funktionale Anforderungen bzw. Eigenschaften, die das Smart Meter Gateway zusätzlich aufweisen muss, finden sich dann in Kapitel 6 „Nicht-Funktionale Anforderungen“.

1.7 Zusammenhang mit anderen Technischen Richtlinien

Die Richtlinie [BSI TR-03109-2] beschreibt das Sicherheitsmodul des Smart Meter Gateways und die von ihm bereitzustellende Funktionalität. Die Richtlinie [BSI TR-03109-3] macht Vorgaben an

die einzusetzenden kryptographischen Verfahren. Die Richtlinie [BSI TR-03109-4] definiert die den Sicherheitsmechanismen zugrunde liegende Zertifikatsinfrastruktur und die dort ablaufenden Prozesse.

1.8 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

2 Technische Einleitung

Das gesamte Kapitel 2 hat informativen Charakter.

Das Kapitel beschreibt einleitend die Funktionalität der Kommunikationseinheit eines intelligenten Messsystems und ihre Einbettung in das technische und organisatorische Umfeld. Die Kommunikationseinheit wird im Folgenden mit dem englischen Terminus „Smart Meter Gateway“ (SMGW) bezeichnet.

Des Weiteren beschreibt dieses Kapitel die Zielsetzung von intelligenten Messsystemen (Kapitel 2.1), die berechtigten Rollen am Smart Meter Gateway (Kapitel 2.2) sowie die Funktionalität des Smart Meter Gateways (Kapitel 2.3).

2.1 Zielsetzung von intelligenten Messsystemen

Im Zuge der Einrichtung von intelligenten Netzen (Smart Grids) werden intelligente Messsysteme (Smart Metering Systems) nach neuem Energiewirtschaftsgesetz (EnWG) zum Einsatz kommen. Durch die Nutzung dieser gesetzlich vorgeschriebenen, in ein Kommunikationsnetz eingebundenen Messsystem, erhalten Letztverbraucher eine höhere Transparenz über den eigenen Energieverbrauch und die Möglichkeit, das eigene Verbrauchsverhalten zu analysieren, um entsprechend die Energiekosten über den laufenden Verbrauch zu senken. Mit Hilfe moderner Tarife, die über das Messsystem abgebildet und ermöglicht werden, können Letztverbraucher ihren Energieverbrauch intelligent gestalten.

Aufgrund der Verarbeitung und Zusammenführung personenbezogener Verbrauchsdaten im SMGW und dem hohen Angriffspotenzial und Ausforschungspotenzial über das angebundene Weitverkehrsnetz, ergeben sich hohe Anforderungen an den Datenschutz und die Datensicherheit. Diese Sicherheitsanforderungen wurden im Rahmen eines Schutzprofils für das Smart Meter Gateway [GW_PP] konkretisiert, das in der Sicherheitsarchitektur eines intelligenten Messsystems die Schlüsselrolle einnimmt.

Aufgrund der Verarbeitung und Zusammenführung personenbezogener Verbrauchsdaten im SMGW und dem hohen Angriffspotenzial und Ausforschungspotenzial über das angebundene Weitverkehrsnetz, ergeben sich hohe Anforderungen an den Datenschutz und die Datensicherheit. Diese Sicherheitsanforderungen wurden im Rahmen eines Schutzprofils für das Smart Meter Gateway [GW_PP] konkretisiert, das in der Sicherheitsarchitektur eines intelligenten Messsystems die Schlüsselrolle einnimmt.

Aufgrund der Erfassung, Zeitstempelung und Verarbeitung von Messwerten unterliegt das Smart Meter Gateway des intelligenten Messsystems eichrechtlichen Vorgaben [Derzeit PTB A50.7 ff].

2.2 Berechtigte Rollen am Smart Meter Gateway

Das Schutzprofil und die Technische Richtlinie beschreiben in ihren Ausführungen technische Rollen, die mit dem SMGW interagieren. Die genaue Definition und Festlegung von Zuständigkeiten von bestehenden Marktrollen ist nicht Teil dieser TR, sondern ergibt sich aus dem Rechtsrahmen.

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

Letztverbraucher (Consumer)

Der Letztverbraucher ist die natürliche oder juristische Person, die elektrische Energie, Gas, Wasser oder Wärme bezieht, bzw. mittels eines lokalen, dezentralen Erzeugers produziert. Der Letztverbraucher ist Eigentümer der im SMGW verarbeiteten und gespeicherten Messwerte. Er kann diese an einer am SMGW vorgesehenen Schnittstelle abrufen (siehe Kapitel 3.4.2.1).

Autorisierte Externe Marktteilnehmer (Authorized External Entity)

Autorisierte externe Marktteilnehmer (EMT) sind aus Sicht des SMGW alle Teilnehmer mit Ausnahme des Smart Meter Gateway Administrators im Weitverkehrsnetz, mit denen das SMGW eine Kommunikation zum Austausch von Daten aufnehmen kann. Hierunter fallen z.B. der Verteilnetzbetreiber (VNB), der Messstellenbetreiber (MSB), der Messdienstleister (MDL), der Lieferant (LF) und sonstige autorisierte Dienstleister.

Smart Meter Gateway Administrator

Der SMGW Administrator (SMGW Admin) ist die vertrauenswürdige Instanz, die das SMGW konfiguriert, überwacht und steuert. Er erstellt und administriert die in das SMGW eingespielten Profile zur Tarifierung, Bilanzierung und Netzzustandsdatenerhebung (siehe Kapitel 4.4) und führt bei Bedarf die Aktualisierung der SMGW-Software durch (siehe Kapitel 3.2.2, Anwendungsfall Firmware Update). Ein SMGW Admin stellt eine gesonderte Rolle im Weitverkehrsnetz dar und ist nicht als externer Marktteilnehmer zu sehen. Das SMGW stellt für die Administration eine Schnittstelle ins Weitverkehrsnetz zur Verfügung.

Service-Techniker

Der Service-Techniker kann vor Ort im Wirkbetrieb eine lokale Diagnoseschnittstelle am SMGW nutzen, um lesenden Zugriff auf das System-Logbuch und weitere Diagnosedaten zu erhalten.

Die hier definierten Rollen sind Akteure im SMGW-Betrieb. In weiteren Phasen des Lebenszyklus können weitere Rollen involviert sein.

2.3 Funktionalität des Smart Meter Gateways

Abgeleitet von der Systemarchitektur, die auf den Vorgaben des Schutzprofils [GW_PP] beruht, muss ein Smart Meter Gateway mindestens drei physische Schnittstellen bereitstellen, wie in Abbildung 1 dargestellt.

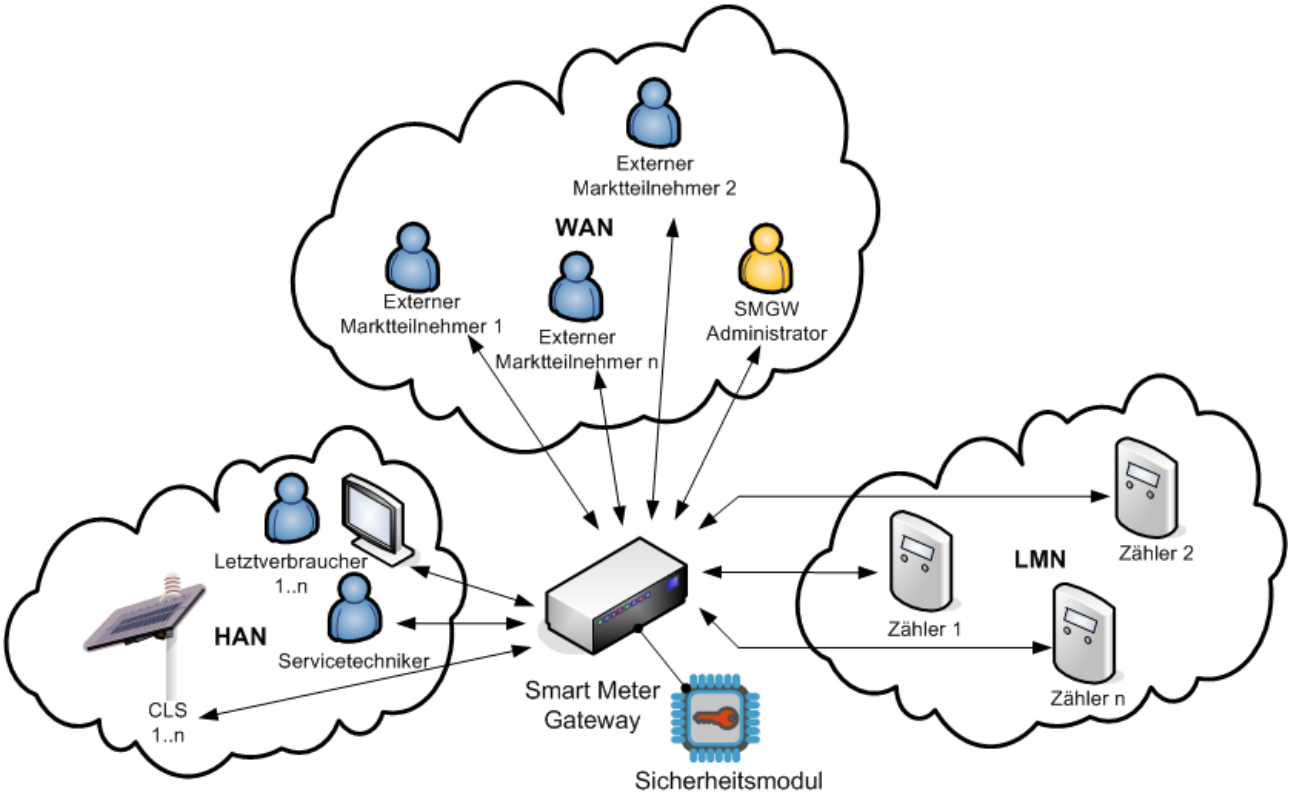

Abbildung 1: Einbettung des Smart Meter Gateways in seine Einsatzumgebung

Folgende Kommunikationsbereiche werden betrachtet:

- das Lokale Metrologische Netz (Local Metrological Network, LMN),

  Im LMN kommuniziert das SMGW mit den angebundenen Zählern für Stoff- und Energiemengen (Strom, Gas, Wasser, Wärme) eines oder mehrerer Letztverbraucher. Die Zähler kommunizieren ihre Messwerte über das LMN an das SMGW.

- das Weitverkehrsnetz (Wide Area Network, WAN),

  Im WAN kommuniziert das SMGW mit den externen Marktteilnehmern und insbesondere auch mit dem SMGW Administrator.

- das Heimnetz (Home Area Network, HAN)

  Im HAN des Letztverbrauchers kommuniziert das SMGW mit den steuerbaren Energieverbrauchern bzw. Energieerzeugern (Controllable Local Systems, CLS, also z.B. intelligente Haushaltsgeräte, Kraft-Wärme-Kopplung- oder Photovoltaik-Anlagen, Stromunterbrecher). Des Weiteren stellt das SMGW Daten für den Letztverbraucher bzw. für den Service-Techniker im HAN bereit.

Das Smart Meter Gateway kommuniziert intern mit seinem Sicherheitsmodul, das als CC-zertifizierte Teilkomponente (siehe [SM_PP]) 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 Regelwerke und der Versendung der verarbeiteten Messwerte an berechtigte Marktteilnehmer im WAN. Messwerte können durch das SMGW

sternförmig an die jeweiligen Adressaten im WAN direkt verteilt werden, aber auch eine indirekte Verteilung über einen bestimmten Marktakteur ist nicht ausgeschlossen.

Daneben bietet das SMGW Funktionen für Letztverbraucher bzw. Service-Techniker, damit diese an der HAN Schnittstelle lesend Verbrauchsdaten bzw. Systeminformationen abrufen können. Für im HAN angeschlossene steuerbare Systeme (CLS) fungiert das SMGW als transparenter Proxy-Server. TLS-geschützte Kommunikationskanäle in Richtung zum CLS und zum externen Marktteilnehmer werden im SMGW terminiert und das SMGW übernimmt die transparente Weiterleitung der jeweils empfangenen Daten.

Gemäß [GW_PP] erfüllt das SMGW die Aufgaben einer Firewall und separiert die angebundenen Netze voneinander. Als dezentraler Speicher personenbezogener Messwerte, die nur gemäß vertraglich vereinbarten Regelungen an berechtigte Parteien versendet werden, stellt das SMGW Datenschutz und Datensicherheit für den Letztverbraucher sicher.

2.3.1 Funktionen des Smart Meter Gateways für das lokale metrologische Netz

Das SMGW kommuniziert mit Zählern ausschließlich im lokalen metrologischen Netz und ist für den Empfang, die Verarbeitung, Speicherung und Versendung von Messwerten und ggf. Netzzustandsdaten verantwortlich. Die lokal angeschlossenen Zähler sind dem SMGW in Form von entsprechenden Zählerprofilen durch den SMGW Administrator bekannt gemacht worden (siehe Kapitel 4.4.2).

Die sichere Kommunikation mit den Zählern erfolgt mit Hilfe der in Kapitel 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. Nach erfolgreicher Entschlüsselung und Integritätsprüfung der Messwerte versieht das SMGW diese mit einem Zeitstempel, der von der Systemuhr des SMGW bereitgestellt wird, und speichert sie in Messwertlisten.
3. Aus bestimmten Messwerten ermittelt das SMGW mit Hilfe eines Regelwerks abgeleitete Messwerte und versendet diese verarbeiteten Werte an berechtigte externe Marktteilnehmer.

Der Vorgang der Zuordnung eines (abgeleiteten) Messwertes zu einer Tarifstufe wird in dieser TR als Tarifierung bezeichnet (siehe dazu auch Kapitel 4.3.3).

Das SMGW unterliegt wegen der durchgeführten Zeitstempelung und Tarifierung der Messwerte dem Eichrecht.

2.3.2 Funktionen des Smart Meter Gateways im Weitverkehrsnetz

Die Verbindung des SMGW zu den externen Marktteilnehmern geschieht über eine WAN-Verbindung.

Die Absicherung der Kommunikation erfolgt mittels der in Kapitel 3.2 festgelegten Protokolle.

Das SMGW besitzt im WAN eine vertrauenswürdige Instanz, den SMGW Administrator (siehe Kapitel 2.2), der das SMGW administriert und wartet.

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

Übertragung der Messwerte anhand von Auswertungs- und Kommunikationsprofilen

Im SMGW werden vom SMGW Administrator Regelwerke in Form von Auswertungsprofilen hinterlegt (siehe Kapitel 4.4.3 dieses Dokuments und Kapitel 1.4.6.1 in [GW_PP]), die die Weiterverarbeitung der empfangenen Messwerte beschreiben. Letzter Schritt dieser Verarbeitung ist die Auslieferung der Daten an berechtigte externe Marktteilnehmer im WAN. Die Verbindungsparameter für die Übertragung der Messwerte hat das SMGW in Kommunikationsprofilen gespeichert.

Pseudonymisierung

Bei der Übertragung von nicht abrechnungsrelevanten Messwerten vom SMGW an einen Marktteilnehmer ist es notwendig, die Identität des Anschlussnutzers (hier gegeben durch die Identität des messenden Zählers) nicht offen zu legen. Um dies zu erreichen, wird die im Datensatz enthaltene Identifikation des Zählers durch ein Pseudonym ersetzt. Damit auch die Identität des sendenden SMGW unerkannt bleibt, müssen die Daten zusätzlich über einen Dritten (den SMGW Administrator) an den Endempfänger vermittelt werden (siehe Kapitel 3.2.4.3).

Beim Versand von Netzzustandsdaten an externe Marktteilnehmer kann bei entsprechender Zweckbindung auf Pseudonymisierung verzichtet werden.

Empfang von Administrations- und Konfigurationsinformationen

Das SMGW wird vom SMGW Administrator konfiguriert und administriert. Dazu sendet der SMGW Administrator Konfigurationsinformationen (siehe Kapitel 4.4) und Befehle, die vom SMGW empfangen und verarbeiten werden.

Firmware Update

Gemäß [GW_PP] unterstützt das SMGW ein Firmware Update. Den Befehl dazu erhält das SMGW vom SMGW Administrator. Die Applikationsdaten im SMGW (z.B. Messwertlisten, Zählerprofile,

Auswertungsprofile, Kommunikationsprofile) dürfen durch ein Firmware Update nicht verändert oder gelöscht werden. Der Updateprozess selbst ist nach [GW_PP] „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 SMGW Administrator bereit. Der SMGW Administrator kann mithilfe des Wake-Up Service das SMGW auffordern eine Kommunikationsverbindung aufzubauen. Beim Wake-Up Service empfängt das SMGW ein spezielles vom SMGW Administrator signiertes Datenpaket (siehe Kapitel 3.2.5). Nach erfolgreicher Verifikation dieses einzelnen Paketes baut das SMGW eine fest vorkonfigurierte Verbindung zum SMGW Administrator auf. Dieser kann über die nun etablierte Verbindung weitere Administrationsbefehle ausführen.

2.3.3 Funktionen des Smart Meter Gateways 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 des Anschlussnutzers (z.B. intelligente Hausgeräte, Photovoltaikanlagen, Klimaanlagen, Mehrwertdienste) gesicherte Kommunikationsverbindungen mit externen Marktteilnehmern im WAN unterhalten (siehe [GW_PP] Kapitel 1.4.6.4). Das SMGW stellt dazu jeweils TLS-gesicherte Verbindungen zu CLS und 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.

Letztverbraucher-Schnittstelle (IF_GW_CON)

Das SMGW bietet berechtigten Letztverbrauchern mit Hilfe der Letztverbraucher-Schnittstelle (IF_GW_CON) [GW_PP] die Möglichkeit, im SMGW für den jeweiligen Letztverbraucher 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 oder ein anderes (CLS-)Gerät im HAN Bereich genutzt werden, welches den kryptographisch gesicherten Datenstrom verarbeiten kann.

Service-Techniker-Schnittstelle (IF_GW_SRV)

Der Service-Techniker kann diese logische Schnittstelle nutzen, um z.B. Konfigurationsprofile und das System-Log einzusehen. Dies unterstützt ihn bei der Diagnose von Fehlersituationen.

2.3.4 Weitere Funktionen des Smart Meter Gateways

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

Nutzerverwaltung/Mandantenfähigkeit

Das SMGW muss die Messwerte von Zählern verschiedener Letztverbraucher (bspw. in Mehrfamilienhäusern) erfassen und speichern können. Dazu hat das SMGW Mechanismen implementiert, um die Multi-Mandantenfähigkeit und die damit verbundenen Authentifizierungsanforderungen (siehe [GW_PP] Kapitel 1.4.6.6) umsetzen zu können.

Zeitsynchronisation

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

Die Synchronisation der SMGW-Systemuhr mit einer zuverlässigen externen Zeitquelle geschieht gemäß den Vorgaben aus Kapitel 3.2.6.

Kryptographische Funktionen

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

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

Protokollierung

Das SMGW protokolliert seine Aktionen in drei unterschiedlichen Log-Bereichen, im System-Log, Letztverbraucher-Log sowie im eichtechnischen Logbuch.

- *System-Log*

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

- *Letztverbraucher-Log*

  Alle Transaktionen des SMGW, z.B. das Versenden von Messwerten, und Aktivitäten des SMGW Administrators werden in einem Letztverbraucher-Log festgehalten. Ein authentifizierter und autorisierter Letztverbraucher 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 einem SMGW Administrator der Zugriff auf das Letztverbraucher-Log nicht erlaubt.

- *Eichtechnisches Logbuch*

  Im eichtechnischen Logbuch werden eichtechnisch relevante Ereignisse (z.B. erkannte Verfälschungen von Messungen, fehlgeschlagene Zeitsynchronisierungen) aufgezeichnet. Au-

ßerdem erfolgt hier die Registrierung von Änderungen an eichtechnisch relevanten Parametern (z.B. das Stellen der Geräteuhr). Dieses Log kann nur von dem autorisierten SMGW Administrator eingesehen werden und wird bei Bedarf vom SMGW Administrator den Eichbehörden zur Verfügung gestellt.

Aufbau und syntaktische Struktur der Logdaten werden in Kapitel 5.2 festgelegt.

3 Anforderungen an die Kommunikationsverbindungen und Protokolle des Smart Meter Gateways

3.1 Einleitung

Dieses Kapitel (Kapitel 3.1) hat informativen Charakter.

Das SMGW verfügt über Schnittstellen zum WAN, HAN und LMN (siehe Abbildung 1), um mit unterschiedlichen Marktteilnehmer und Geräten in diesen Netzen zu kommunizieren.

Die folgenden Kapitel legen die Anforderungen an die Kommunikation im WAN (siehe Kapitel 3.2), LMN (siehe Kapitel 3.3) und HAN (siehe Kapitel 3.4) zu den verschiedenen Marktteilnehmern und Komponenten in diesen Netzen fest.

3.2 Vorgaben an die Kommunikationsverbindungen im WAN

3.2.1 Übersicht

Dieses Kapitel (3.2.1) hat informativen Charakter.

Anwendungsfälle, die eine WAN Kommunikation erfordern, werden in Kapitel 3.2.2 kurz skizziert. Zur Realisierung dieser Anwendungsfälle werden mehrere Kommunikationsszenarien herangezogen, welche vom SMGW unterstützt werden müssen. Diese werden in Kapitel 3.2.3 definiert.

Die Anforderungen an die konkrete Umsetzung der Kommunikationsszenarien auf Ebene der Kommunikationsprotokolle mit Hilfe von Webservices erfolgt in Kapitel 3.2.4.

Festlegungen zum „Wake-Up Service“ erfolgen in Kapitel 3.2.5 und die Synchronisation der Zeit im SMGW wird in Kapitel 3.2.6 spezifiziert.

3.2.2 Anwendungsfälle an der WAN Schnittstelle

Dieses Kapitel listet diejenigen Anwendungsfälle auf (gekennzeichnet mit dem Kürzel WAF-*), die zwingend eine Kommunikation des SMGW mit Teilnehmern im WAN erfordern. Das SMGW **MUSS** mindestens diese Anwendungsfälle unterstützen.

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

1. Administration und Konfiguration des Smart Meter Gateways durch den SMGW Administrator
2. Zugriff des SMGW auf Dienste beim SMGW Administrator
3. Alarmierung und Benachrichtigung des SMGW Administrators bei Auftreten von (unerwarteten) Ereignissen im SMGW
4. Übertragung von Daten an den SMGW Administrator.

Die übertragenen Daten können entweder für den SMGW Administrator bestimmt sein oder auch für einen Dritten. Dies ist z.B. bei der pseudonymisierten Übertragung von Netzzustandsdaten der Fall.

5. Übertragung von Daten an externe Marktteilnehmer
6. Kommunikation externer Marktteilnehmer mit einem CLS über das SMGW (siehe Kapitel 3.4)
7. Wake-Up Service (siehe Kapitel 3.2.5)

WAF1: Administration und Konfiguration

Das SMGW **MUSS** ausschließlich durch den SMGW Administrator administriert werden. Eine Administration durch Dritte **DARF NICHT** möglich sein. Für die Administration durch den SMGW Administrator **MUSS** das SMGW mindestens die folgenden Dienste bereitstellen:

- Geräteverwaltung

  Im SMGW **MÜSSEN** Geräte (Zähler, CLS, Anzeigeeinheiten) durch den SMGW Administrator registriert und einem Letztverbraucher zugeordnet werden können.

- Mandantenverwaltung

  Im SMGW **MÜSSEN** durch den SMGW Administrator Letztverbraucher angelegt, bearbeitet, gelöscht und zugeordnete Zertifikate bzw. Userid/Passwort eingerichtet oder gelöscht werden können.

- Profilverwaltung

  In das SMGW **MÜSSEN** durch den SMGW Administrator Zählerprofile, Kommunikationsprofile und Auswertungsprofile z.B. zur Tarifierung und Netzzustandsmeldung eingebracht, aktiviert und gelöscht werden können.

- Schlüssel-/Zertifikatsmanagement

  In das SMGW **MÜSSEN** durch den SMGW Administrator Schlüssel und Zertifikate für die Kommunikation mit Zählern, CLS, externen Marktteilnehmern eingebracht, aktiviert, deaktiviert bzw. gelöscht werden können.

- Firmware Update

  Das SMGW **MUSS** es dem SMGW Administrator erlauben, neue Firmware in das SMGW aufzuspielen, zu verifizieren und zu aktivieren. Diese **MUSS** über Mechanismen verfügen anhand derer eine Verifikation der Integrität möglich ist, bevor eine Aktivierung erfolgen kann.

- Wake-Up Konfiguration

Das SMGW **MUSS** es dem SMGW Administrator erlauben, die Adresse des Wake-Up Service zu konfigurieren.

- SMGW Monitoring

  Das SMGW **MUSS** es dem SMGW Administrator erlauben, den Zustand des SMGW abzufragen und Logeinträge aus dem System- und eichtechnischen Log auszulesen.

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

Das Kommunikationsszenario, dem dieses Kommunikationsmuster zugrunde liegt, wird im Folgenden als „MANAGEMENT“ bezeichnet.

WAF2: Zugriff auf Dienste beim SMGW Administrator

Dienste, auf die das SMGW im Betrieb angewiesen ist, **MUSS** das SMGW beim SMGW Administrator aufrufen können. Beispiele sind:

- Zeitsynchronisation

  Das SMGW **MUSS** seine Systemzeit mit einem vertrauenswürdigen Zeitdienst beim SMGW Administrator synchronisieren.

- Firmware Download

  Das SMGW **KANN** einen Dienst beim SMGW Administrator nutzen, um neue Firmware herunterzuladen. Dies **MUSS** nur auf Befehl des SMGW Administrators erfolgen. Ein Soft- oder Firmwareupdaten von anderen Parteien, **DARF NICHT** möglich sein.

- Auslieferung von tarifierten Messwerten oder Netzzustandsdaten

  Das SMGW **MUSS** einen Dienst beim SMGW Administrator nutzen können, um tarifierte Messwerte oder Netzzustandsdaten an den SMGW Administrator auszuliefern, die dieser dann an einen EMT weiterleitet.

Das Kommunikationsszenario, dem dieses Kommunikationsmuster zugrunde liegt, wird im Folgenden als „ADMIN-SERVICE“ bezeichnet.

WAF3: Alarmierung und Benachrichtigung

Während des Betriebs des SMGW können unerwartete Ereignisse oder Fehlersituationen auftreten, die zur Analyse und weiteren Bearbeitung an den SMGW Administrator gemeldet werden **MÜSSEN**. Ebenso **KANN** das SMGW regelmäßig Benachrichtigungen an den SMGW Administrator senden (z.B. jeden Tag eine „Alive“ Nachricht).

Damit das SMGW solche Nachrichten an den SMGW Administrator übermitteln kann, **MUSS** das SMGW einen Dienst beim SMGW Administrator aufrufen, der die Zustellung solcher Ereignisse durch das SMGW ermöglicht. Diese Anwendungsfälle werden demnach dem Kommunikationsszenario „ADMIN-SERVICE“ zugeordnet.

WAF4: Übertragung von Daten an den SMGW Administrator

Die Übertragung von Daten an den SMGW Administrator **MUSS** durch den Aufruf eines Dienstes beim SMGW Administrator erfolgen und fällt somit in die Kategorie „ADMIN-SERVICE“.

WAF5: Übertragung von Daten an externe Marktteilnehmer

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

- Turnusmäßige Auslieferung von tarifierten Messwerten

  Das SMGW **MUSS** gemäß eines Auswertungsprofils und eines Kommunikationsprofils regelmäßig abrechnungsrelevante Messwerte zur Tarifierung an einen externen Marktteilnehmer ausliefern können.

- Turnusmäßige Netzzustandsdatenauslieferung

  Das SMGW **MUSS** gemäß eines Auswertungs- und Kommunikationsprofils regelmäßig Messwerte zum Netzzustand an einen externen Marktteilnehmer ausliefern können.

- Spontane Messwertauslesung

  Ein externer Marktteilnehmer hat keinen direkten Zugriff auf die Daten des SMGW. Daher **MUSS** die Spontanablesung dadurch nachgebildet werden, dass der SMGW Administrator ein geeignetes Auswertungs- und Kommunikationsprofil in das SMGW einbringt (falls noch nicht vorhanden), das die Auslieferung der benötigten Messwerte an den externen Marktteilnehmer auslöst.

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

Das SMGW **MUSS** die Daten an eine Dienstschnittstelle beim externen Marktteilnehmer übergeben, die die zuverlässige Auslieferung durch das SMGW ermöglicht.

Das Kommunikationsszenario, dem dieses Kommunikationsmuster zugrunde liegt, wird im Folgenden als „INFO-REPORT“ bezeichnet.

WAF6: Kommunikation EMT mit CLS

Das SMGW **MUSS** Anwendungsfälle zur Kommunikation eines externen Marktteilnehmers mit einem CLS Gerät unter Nutzung der TLS Proxy Funktionalität des SMGW unterstützen. Diese Anwendungsfälle werden in Kapitel 3.4 behandelt.

WAF7: Wake-Up Service

Das SMGW **MUSS** den Wake-Up Service implementieren. Dieser Anwendungsfall wird in Kapitel 3.2.5 behandelt

3.2.3 Kommunikationsszenarien

Die in Kapitel 3.2.2 skizzierten Anwendungsfälle an der WAN Schnittstelle, bei denen das SMGW mehr als nur Proxy-Funktionalität anbietet, lassen sich auf folgende fünf Kommunikationsszenarien (gekennzeichnet mit dem Kürzel WKS) abbilden, die vom SMGW unterstützt werden **MÜSSEN**:

- MANAGEMENT (Administration)

  Zugriff des SMGW Administrators auf Services des SMGW, die dieses an seiner WAN-Schnittstelle dem SMGW Administrator anbietet.

- ADMIN-SERVICE

  Zugriff des SMGW auf Services des SMGW Administrators, die dieser an seiner WAN-Schnittstelle dem SMGW anbietet.

- INFO-REPORT

  Zugriff des SMGW auf Services des externen Marktteilnehmers zum Versand von Daten durch das SMGW an den externen Marktteilnehmer.

- NTP-HTTPS

  Zeitsynchronisierung über einen vom SMGW Administrator bereitgestellten Web-Service.

- NTP-TLS

  Zeitsynchronisierung über einen vom SMGW Administrator bereitgestellten NTP-Service.

Szenario	**Typ**	**Service Requester**	**Service Provider**	**TLS Endpunkt**	**PointOfContact[1] beim Service Provider**
WKS1	MANAGEMENT	SMGW Administrator	SMGW	SMGW Administrator	/smgw/cosem/…
WKS2	ADMIN-SERVICE	SMGW	SMGW Administrator	SMGW Administrator	/gwa/… <Service PoC>

[1] Point of Contact (PoC) bezeichnet den URI Präfix, der zur URI Adressierung eines Service beim Service Provider vorangestellt werden muss. Durch ihn wird der gewünschte Webservice selektiert.

Szenario	Typ	Service Requester	Service Provider	TLS Endpunkt	PointOfContact[1] beim Service Provider
WKS3	INFO-REPORT	SMGW	EMT	EMT	/<emt>[2]/… <Report PoC>
WKS4	NTP-HTTPS	SMGW	SMGW Administrator	SMGW Administrator	-
WKS5	NTP-TLS	SMGW	SMGW Administrator	SMGW Administrator	

Tabelle 1: Kommunikationsszenarien an der WAN Schnittstelle

Innerhalb einer TLS Verbindung des SMGW **MUSS** genau ein Kommunikationsszenario ablaufen. Ein Wechsel des Kommunikationsszenarios während einer bestehenden TLS Verbindung **DARF NICHT** vorgenommen werden. Das SMGW **MUSS** zwei parallele TLS Verbindungen zum SMGW Administrator unterhalten können**;** eine „MANAGEMENT-Verbindung“ und eine „ADMIN-SERVICE“ Verbindung.

Das SMGW **MUSS** für WKS1 und WKS2 unterschiedliche Adressen auf Transportebene für den SMGW Administrator konfigurieren, damit dieser unterscheiden kann, ob die aufgebaute TLS Verbindung vom Typ MANAGEMENT oder ADMIN-SERVICE ist.

Eine Ausnahme ist die Verwendung des Kommunikationsszenarios WKS4 (NTP-HTTPS) innerhalb einer TLS-Verbindung für das Kommunikationsszenario WKS2 (ADMIN-SERVICE). WKS4 verwendet in diesem Kommunikationsszenario kein CMS.

3.2.3.1 MANAGEMENT

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

[2] <emt> in spitzen Klammern ist ein Platzhalter für einen vom EMT festgelegten URI Präfix

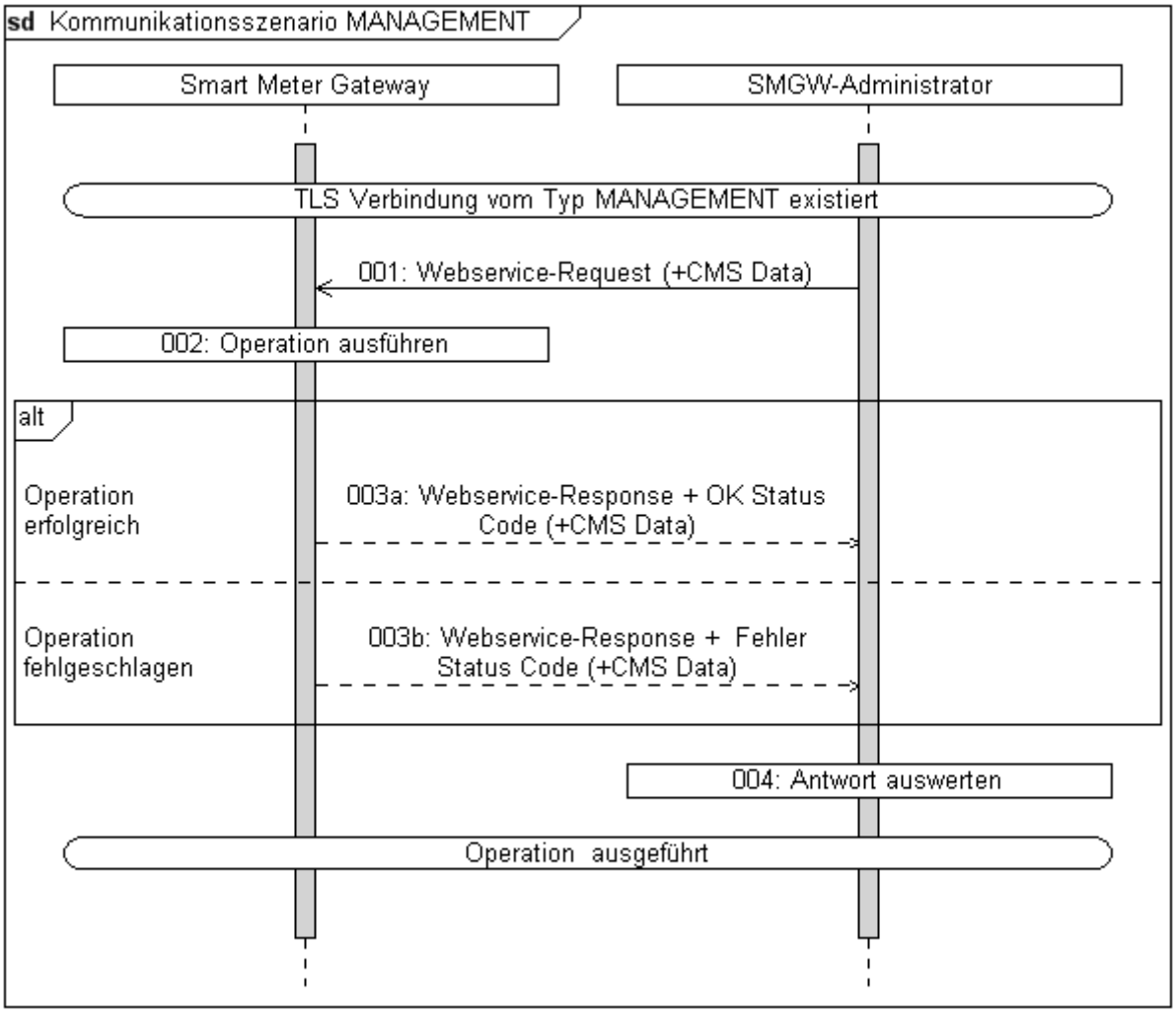

Abbildung 2: Einbettung des Smart Meter Gateways in seine Einsatzumgebung

Vorbedingung:

Es besteht eine TLS-Verbindung zwischen SMGW und SMGW Administrator vom Typ MANGEMENT. Der Point of Contact zum Zugriff auf Management-Services beim SMGW ist dem SMGW Administrator bekannt.

Rolle des Smart Meter Gateways:

Server

Step	Event	Process/Activity	Info Producer	Info Receiver	Data Exchanged.
001		SMGW-Admin erstellt und sendet Webservice-	SMGW Admin	SMGW	Webservice-Request

		Request			(+CMS-Daten)
002	SMGW empfängt Webservice-Request	SMGW führt Operation aus			
003a	Operation erfolgreich beendet	SMGW sendet Webservice-Response an SMGW Administrator	SMGW	SMGW Admin	Webservice-Response-Code OK (+ CMS-Data)
003b	Operation nicht erfolgreich beendet	SMGW sendet Webservice-Response an SMGW Administrator	SMGW	SMGW Admin	Webservice-Response mit Fehler Code (+ CMS-Data)
004	SMGW Administrator empfängt Response	SMGW Administrator verarbeitet Response			

Tabelle 2: Beschreibung Kommunikationsszenario „MANAGEMENT“

3.2.3.2 ADMIN-SERVICE

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

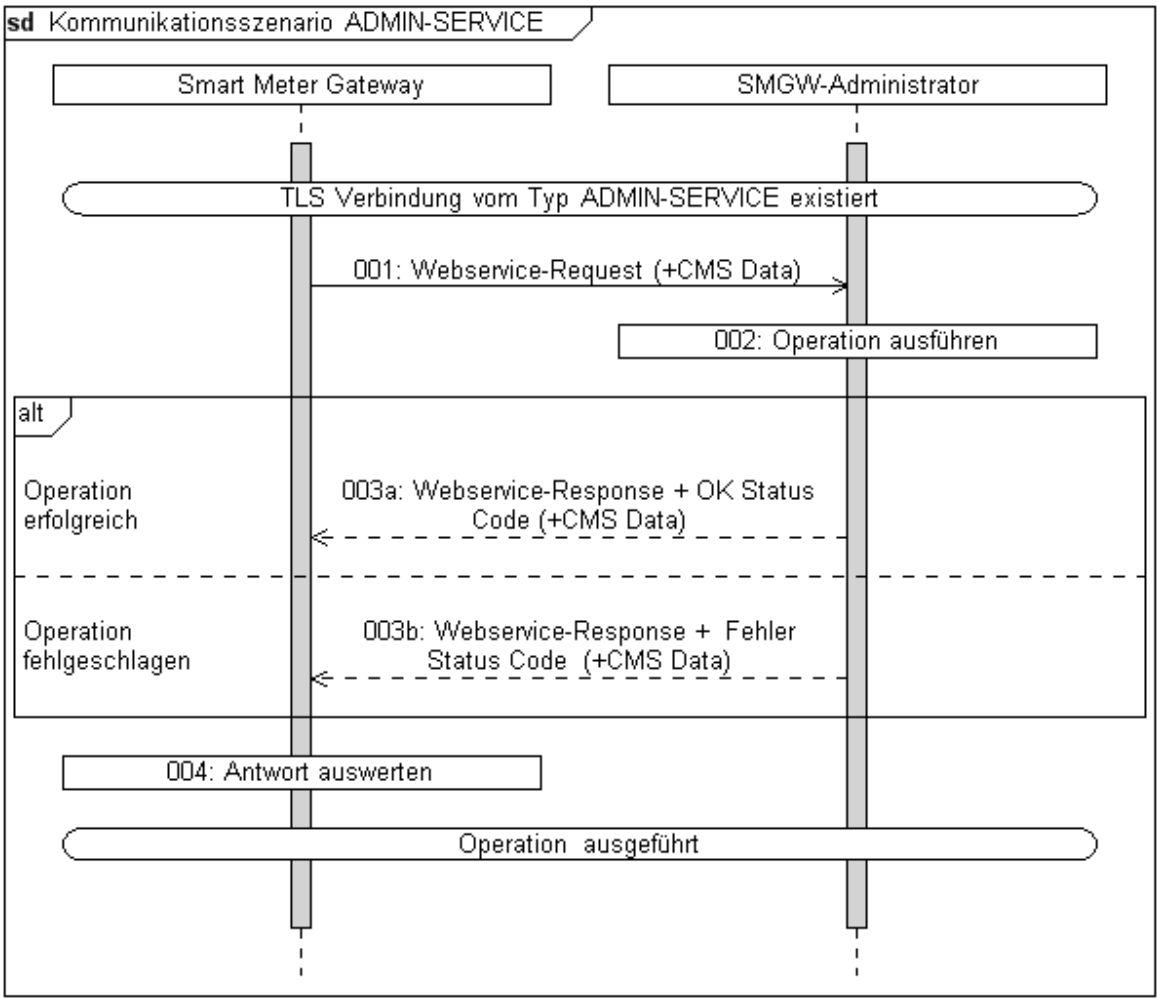

Abbildung 3: Sequenzdiagramm Kommunikationsszenario „ADMIN-SERVICE“

Vorbedingung:

Es besteht eine TLS-Verbindung zwischen SMGW und SMGW Administrator vom Typ ADMIN-SERVICE. Der Point of Contact zum Zugriff auf Admin-Services beim SMGW Administrator ist dem SMGW bekannt.

Rolle des Smart Meter Gateways:

Client

Step	Event	Process/Activity	Info Producer	Info Receiver	Data Exchanged
001		SMGW sendet Webservice-Request	SMGW	SMGW Administrator	Webservice-Request (+CMS-Data)
002	SMGW Administrator empfängt Request	SMGW Administrator verarbeitet Request-Daten			
003a	Request wurde erfolgreich vom SMGW Administrator verarbeitet	SMGW Administrator sendet Webservice-Response	SMGW Administrator	SMGW	Webservice-Response-Code OK (+ CMS-Data)
003b	Request wurde nicht erfolgreich vom SMGW Administrator verarbeitet	SMGW Administrator sendet Webservice-Response	SMGW Administrator	SMGW	Webservice-Response mit Fehler Code (+ CMS-Data)
004	SMGW empfängt Webservice-Response	SMGW verarbeitet Response			

Tabelle 3: Beschreibung Kommunikationsszenario „ADMIN-SERVICE“

3.2.3.3 INFO-REPORT

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

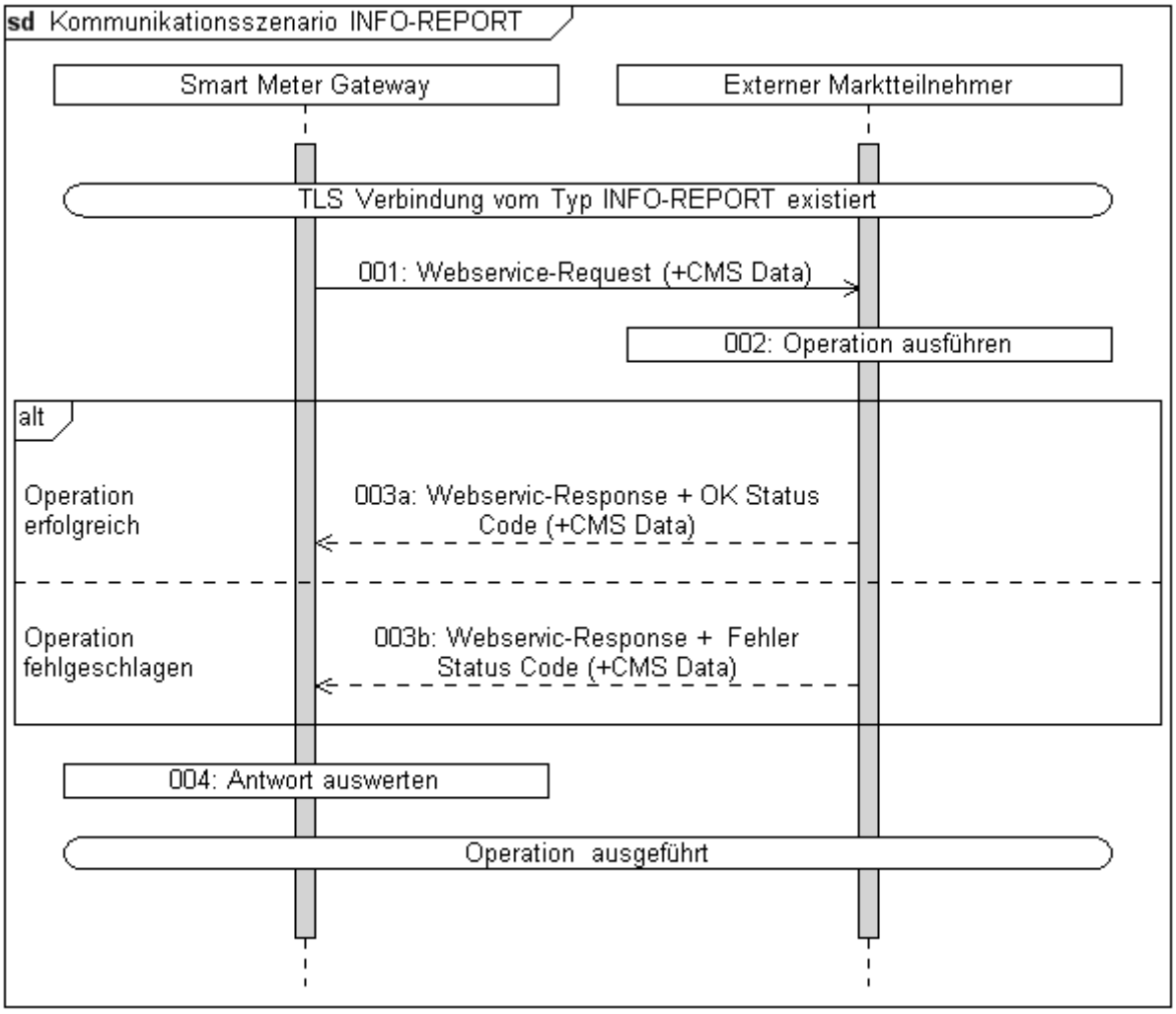

Abbildung 4: Sequenzdiagramm Kommunikationsszenario „INFO-REPORT“

Vorbedingung:

Es besteht eine TLS-Verbindung zwischen SMGW und einem externen Marktteilnehmer vom Typ INFO-REPORT. Der Point Of Contact zum Zugriff auf Info-Report-Services beim externen Marktteilnehmer ist dem SMGW bekannt.

Rolle des Smart Meter Gateways:

Client

Step	Event	Process/Activity	Info Producer	Info Receiver	Data Exchanged
001		SMGW sendet Webservice-Request	SMGW	EMT	Webservice-Request (+CMS-Data)
002	EMT empfängt Request	EMT verarbeitet Request-Daten			
003a	Request wurde erfolgreich vom	EMT sendet Webservice-Response	EMT	SMGW	Webservice-Response-Code

	EMT verarbeitet				OK (+CMS-Data)
003b	Request wurde nicht erfolgreich vom EMT verarbeitet	EMT sendet Webservice-Response	EMT	SMGW	Webservice-Response mit Fehler Code (+CMS-Data)
004	SMGW empfängt Webservice-Response	SMGW verarbeitet Response			

Tabelle 4: Beschreibung Kommunikationsszenario „ADMIN-SERVICE“

3.2.3.4 NTP-HTTPS

Dieses Kommunikationsszenario entspricht WKS2, jedoch ohne CMS. Es wird für den Zeitabgleich über den ADMIN-SERVICE verwendet.

3.2.3.5 NTP-TLS

Vorbedingung:

Es besteht eine TLS-Verbindung zwischen SMGW und SMGW Administrator.

Rolle des Smart Meter Gateways:

Client

Step	Event	Process/Activity	Info Producer	Info Receiver	Data Exchanged
001		SMGW sendet NTP Paket	SMGW	SMGW Administrator	NTP data
002	SMGW Administrator empfängt NTP Paket	SMGW Administrator verarbeitet NTP Paket			
003	NTP Paket wurde erfolgreich vom SMGW Administrator verarbeitet	SMGW Administrator sendet NTP Paket	SMGW Administrator	SMGW	NTP data
004	SMGW empfängt NTP Paket	SMGW verarbeitet NTP Paket			

Tabelle 5: Beschreibung Kommunikationsszenario „NTP-TLS“

3.2.4 RESTful Webservices

Die oben definierten Kommunikationsszenarien sowie die darauf aufsetzenden Dienste und Anwendungsfälle **MÜSSEN** mit Hilfe von Webservices im SMGW, beim SMGW Administrator und beim EMT erbracht werden.

Dieses Kapitel macht deswegen Vorgaben in folgenden Bereichen, die zur Sicherstellung der Interoperabilität bei der WAN Kommunikation notwendig sind:

1. Datenmodellierung
2. Zugriffsprotokoll zur Abfrage und Darstellung der Daten
3. Inhaltsdatensicherung
4. Transferprotokoll und Transportsicherung

Für die Kommunikation des SMGW über das WAN mit dem SMGW Administrator bzw. mit externen Marktteilnehmern **MUSS** folgender Protokollstapel implementiert werden:

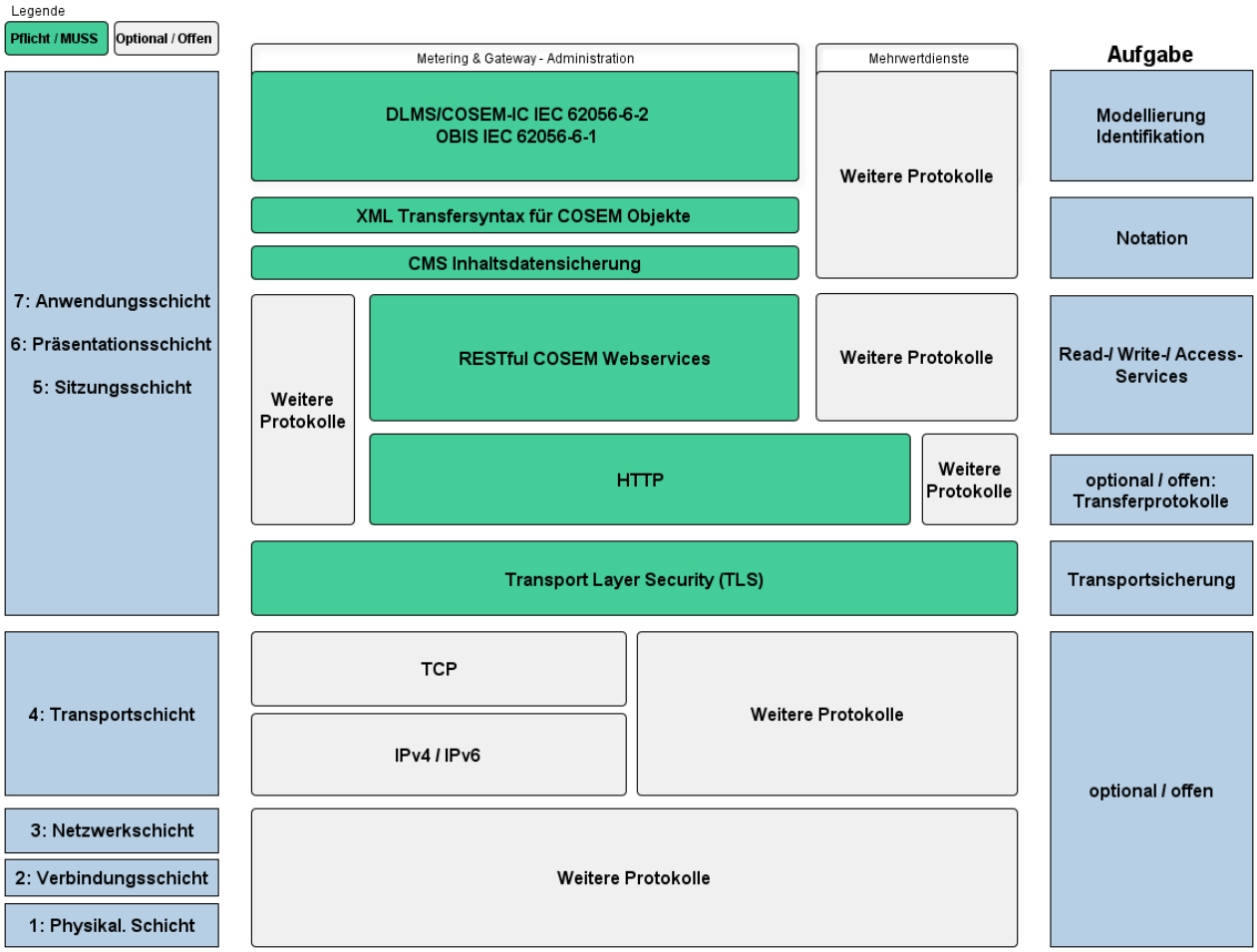

Abbildung 5: Protokollstapel für die WAN Kommunikation

Anmerkung: Die Protokolle unterhalb des TLS-Layers werden von der TR nicht vorgegeben.

3.2.4.1 Datenmodellierung mit COSEM Interface Klassen

Die Modellierung der Datenstrukturen des SMGW für Metering und Administration **MUSS** mit Hilfe von COSEM Interface-Klassen aus dem Standard [IEC 62056-6-1] und den OBIS Codes aus den Standards [IEC 62056-6-2] und [EN 13757-1] geschehen.

Mit Hilfe dieser COSEM Klassen werden die Datenstrukturen, die sich aus den Anwendungsfällen aus Kapitel 3.2.2 ableiten, abgebildet.

3.2.4.2 HTTP als Zugriffsprotokoll auf COSEM Ressourcen

Die Übertragung der COSEM Objekte bzw. die Übertragung von Aggregationen von COSEM Objekten (in „Anlage II: COSEM/HTTP Webservices“ als „Containern“ bezeichnet) sowie der Aufruf von COSEM Objektmethoden **MUSS** mittels Webservices geschehen.

Zum Transport der Webservice Requests und Responses wird HTTP/1.1 gemäß [RFC2616] genutzt. Die Festlegungen zu

- XML Transfersyntax für COSEM Objekte
- Ressourcenbaumstruktur der COSEM Objekte und ihre Adressierung
- Selektiver Zugriff auf Teile von Objektattributen („Selective Access“)
- Zugriffssemantik der HTTP Verben
- Zugriffsrechte
- Blocktransfer
- HTTP Header Fields
- HTTP Status Codes

sind in „Anlage II: COSEM/HTTP Webservices“ spezifiziert.

Das COSEM-Zugriffsprotokoll basiert dabei auf einem RESTful Webservice Designmodell.

Zusätzlich zu der allgemeinen Protokollspezifikation in „Anlage II: COSEM/HTTP Webservices“ **MÜSSEN** zur Interoperabilität die Anforderungen, die in den folgenden Abschnitten beschrieben werden, erfüllt werden.

3.2.4.2.1 Kanonische Geräte-ID und Bezeichner für Container

Zur Adressierung des SMGW und der „Logical Devices“ (d.h. der virtuellen Zähler, siehe Abbildung 6) innerhalb des SMGW **MUSS** eine kanonische Geräte-ID verwendet werden.

Jedes SMGW und jedes „Logical Device“ (virtueller Zähler) hat eine eindeutige herstellerübergreifende Identifikationsnummer nach [DIN 43863-5:2012-04]. Diese Identifikationsnummer wird im Rahmen der Technischen Richtlinie in folgender Form kanonisiert und dient dann als „Hostname“ bzw. als „Logical Device-Name“ innerhalb einer URI:

1. Großbuchstaben werden zu Kleinbuchstaben.
2. Das Suffix „**.sm**“ wird angehängt.

Die resultierende Zeichenfolge enthält nur die Zeichen a-z, 0-9 und Punkt. [3]

Der „Fully Qualified Domain Name (FQDN)“ eines SMGW setzt sich dann aus seiner kanonischen Geräte-ID, den umgebenden Sub-Domänennamen und der Top Level Domain **.de** zusammen, z.B. `1din0063539421.sm.<tbd>.de`.

Um die kanonische Geräte-ID in eine Repräsentation nach [DIN 43863-5:2012-04] zurück zu transformieren **MÜSSEN** die folgenden Schritte ausgeführt werden:

1. Das Suffix „**.sm**“ wird entfernt.
2. Alle Kleinbuchstaben werden zu Großbuchstaben.

Beispiel:

Identifikationsnummer nach [DIN 43863-5:2012-04]	**kanonische Geräte-ID**
1 DIN0063539421	1din0063539421.sm

Tabelle 6: Beispiel „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“.

Eine Nutzung dieses Schemas für andere Identifikationsnummern ist möglich (z.B. MAC-Adressen).

Für Container-Objekte (siehe „Anlage II: COSEM/HTTP Webservices“) **MÜSSEN** OBIS-IDs (z.B. aus einem länder- oder konsortiumzugewiesenen Bereich) verwendet werden. Damit sind die Container innerhalb eines Logical Devices eindeutig adressierbar.

Abbildung 6 zeigt die Nutzung der kanonischen Geräte-ID zur Adressierung eines physikalischen COSEM Devices bzw. zur Adressierung von Logical Devices innerhalb des physikalischen Devices. Die Adressierung eines Containers mittels seiner OBIS-ID ist ebenfalls beispielhaft dargestellt.

[3] 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 SGW-Admin verwaltete feste Zuordnung zwischen Hostnamen und Transportadresse im SMGW ist ebenso möglich.

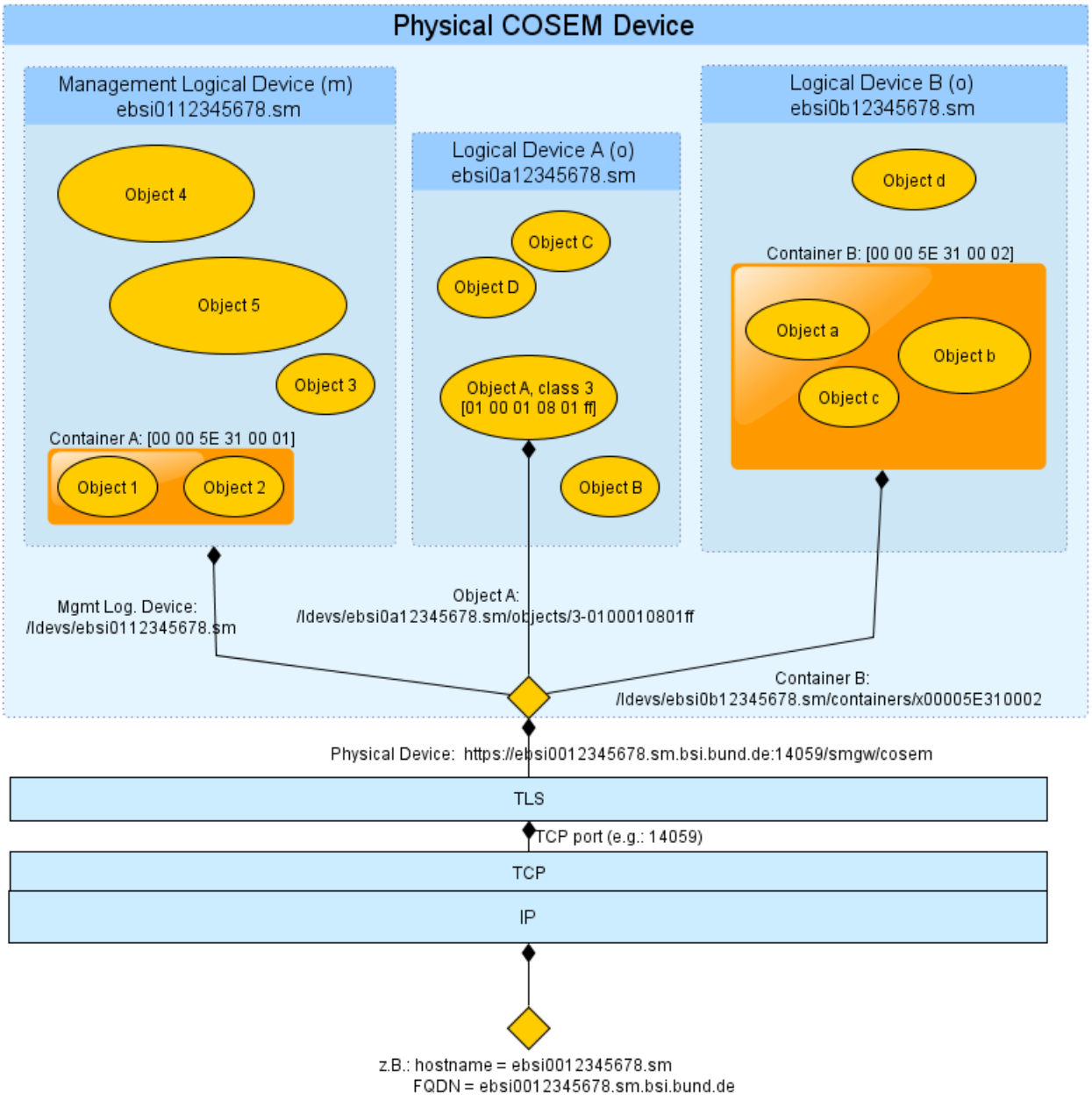

Abbildung 6:URI Adressierung mit kanonischer Geräte-ID

3.2.4.2.2 HTTP Statuscode

Fehlerfälle im SMGW, die bei der Bearbeitung eines HTTP-Request auftreten können, werden mit den in „Anlage II: COSEM/HTTP Webservices“ aufgelisteten HTTP-Statuscodes beantwortet. Die Statuscodes und eventuell als COSEM Objekt im Response Body vorhandene Detailinformation zum aufgetretenen Fehler **MUSS** das SMGW im System Log aufzeichnen.

3.2.4.3 Pseudonymisierung/Anonymisierung

Bei einer pseudonymisierten Übertragung von Messwerten (Netzzustandsdaten) **MUSS** das SMGW die kanonische Geräte-ID des SMGW sowie die kanonische Geräte-ID des Logical Devices, aus dem die Messwerte stammen, durch ein Pseudonym ersetzen. Die kanonischen Geräte-ID-Werte **DÜRFEN** in den (XML-) Inhaltsdaten **NICHT** mehr auftreten.

Die Pseudonymisierung von Netzzustandsdaten bei der Übertragung vom SMGW an einen externen Marktteilnehmer **MUSS** durch die folgenden Schritte sichergestellt werden:

1. Aus Messwerten, die einem Auswertungsprofil folgend pseudonymisiert übertragen werden sollen, wird die eindeutige kanonische Geräte-ID durch das SMGW entfernt und durch ein im Auswertungsprofil hinterlegtes Pseudonym ersetzt.
2. Die so aufbereiteten Daten werden dann vom SMGW für den Empfänger (EMT) verschlüsselt, signiert und an den SMGW Administrator übertragen.
3. Der SMGW Administrator prüft die Signatur des SMGW und damit die Authentizität der empfangenen Daten und leitet diese nach Entfernung der SMGW Signatur an den Empfänger weiter.
4. Der Empfänger entschlüsselt die Nachricht

Die folgende Abbildung skizziert diese Schritte:

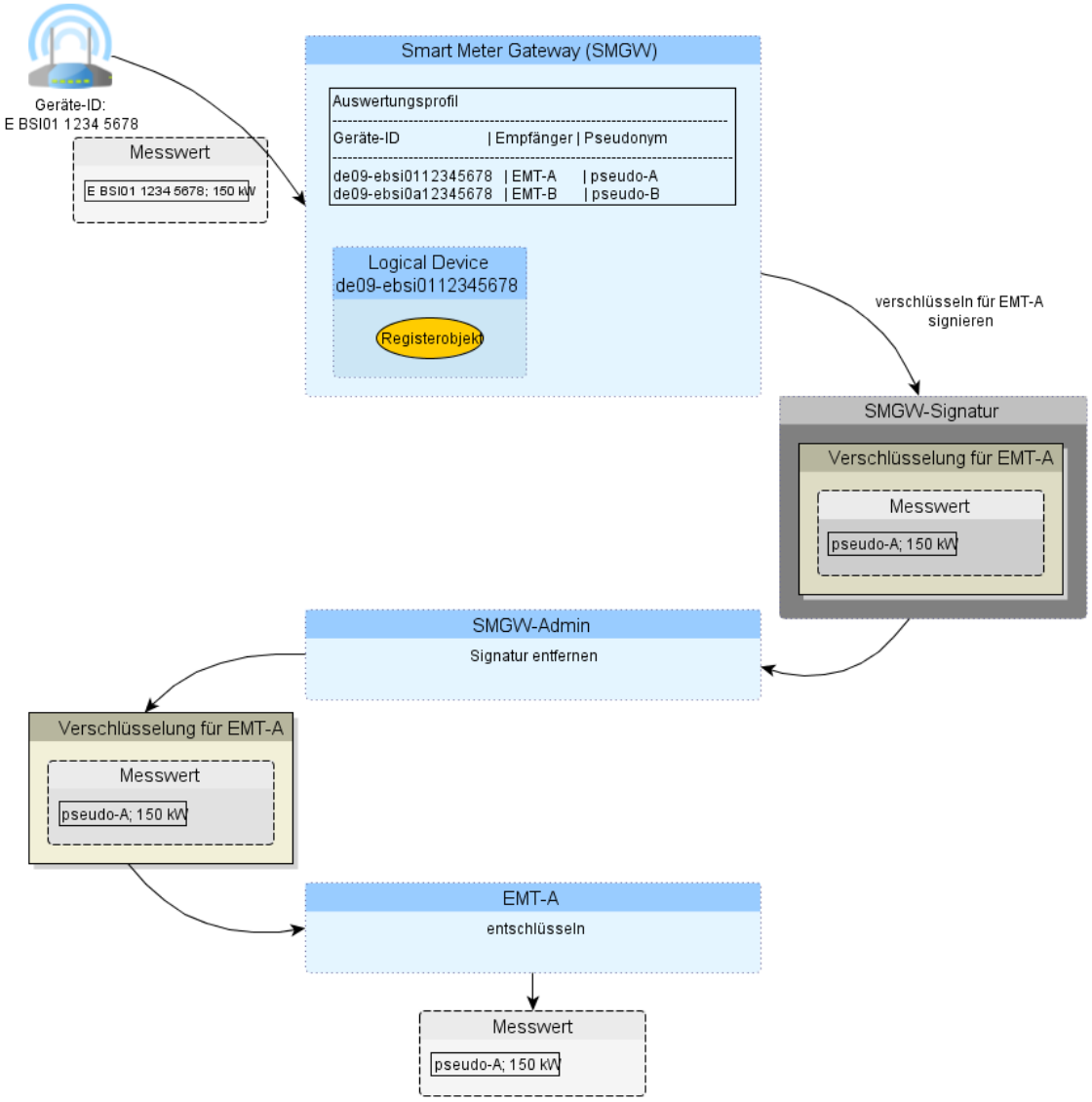

Abbildung 7: Pseudonymisierte Messdatenübertragung

Die Rückverfolgung des Letztverbrauchers anhand der Signatur des sendenden SMGW ist für den Empfänger (im Beispiel: EMT-A) wesentlich erschwert, da die SMGW Signatur vom SMGW Administrator entfernt wurde.

Die Rückverfolgung des Letztverbrauchers über eine kanonische Geräte-ID ist für den Empfänger wesentlich erschwert, da die Daten ein Pseudonym (im Beispiel: pseudo-A) anstelle der kanonischen Geräte-ID enthalten.

3.2.4.4 Inhaltsdatensicherung mittels CMS

Zur Sicherung der Inhaltsdaten im WAN **MÜSSEN** gemäß [GW_PP] die COSEM Objekte bzw. aggregierten Objekt-Container für den Endempfänger verschlüsselt und vom Absender signiert werden.

Der CMS-Container vom ASN.1 Typ „SignedData“, der die Signatur über eine Datenstruktur vom ASN.1 Typ „AuthEnvelopedData“ bildet, **MUSS,** wie in „Anlage I: CMS Datenformat für die Inhaltsdatenverschlüsselung und -signatur“ spezifiziert, erzeugt werden.

Zusätzlich **MÜSSEN** die folgenden Vorgaben für die HTTP Kommunikation erfüllt werden:

1. Für die Kennzeichnung der COSEM-Daten mit XML-Transfersyntax und CMS Inhaltsdatensicherung **MUSS** der Content-Type `application/vnd.de-dke-k461-cosem+xml;encap=cms-tr03109` verwendet werden.
2. Für die Kennzeichnung der CMS-Inhaltsdatenverschlüsselung ohne vorherige Kompression der XML Daten **DARF KEIN** Content-Encoding Header Feld vorhanden sein.
3. Für die Kennzeichnung der CMS-Inhaltsdatenverschlüsselung mit vorheriger Kompression der XML Daten **MUSS** das Content-Encoding `deflate` verwendet werden.
4. Server und Client **MÜSSEN** sowohl komprimierte als auch unkomprimierte CMS-Daten verarbeiten können. Der ASN.1 ContentType des verschlüsselten Inhalts hat den ASN.1-Object Identifier-Wert „`id-data`“ oder „`id-ct-compressedData`“.
5. Requests/Reponses ohne HTTP-Body **DÜRFEN NICHT** mittels Inhaltsdatensicherung abgesichert werden, d.h. Status-Codes über den HTTP-Header werden durch TLS gesichert, aber nicht zusätzlich CMS-verpackt.

Einzelne Attribute von COSEM Objekten (z.B. Messwerte oder Messwertreihen) **KÖNNEN**, je nach Anwendungsfall, zusätzlich vom SMGW signiert werden („innere Signatur“). Für welche Objektattribute diese Signatur erforderlich ist, **MUSS** durch die Modellierung innerhalb einer COSEM Klasse festgelegt werden. Anforderungen dazu sind in Kapitel 4 zu finden.

3.2.4.5 Anforderungen an TLS bei WAN Verbindungen

Gemäß den Anforderungen aus dem Schutzprofil [GW_PP] **MÜSSEN** die Kommunikationsverbindungen des SMGW oberhalb der Transportschicht mittels TLS abgesichert werden.

Für die 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. Dabei **MUSS** immer ein beidseitig auf Zertifikaten basierender authentifizierter TLS-Kanal aufgebaut werden. Die Zertifikate **MÜSSEN** aus der Smart Metering Public Key Infrastruktur [BSI TR-03109-4] stammen.

Das SMGW **DARF KEINE** TLS-Verbindungen akzeptieren, die von Teilnehmern aus dem WAN initiiert werden. Das SMGW kann jedoch für einen bestimmten Fall über den Wake-Up Dienst (siehe Kapitel 3.2.5) veranlasst werden, eine TLS Verbindung zum Smart Meter Gateway Administrator aufzubauen.

Es **MÜSSEN** zu einem Zeitpunkt zwei oder mehr TLS-Verbindungen zwischen SMGW und SMGW Administrator gleichzeitig existieren können (z.B. zum Management des Gateways und zur Fehlersignalisierung bzw. Alarmierung, siehe Kapitel 3.2.3). Die Verbindungen **MÜSSEN** das gleiche Zertifikat und die zugehörigen privaten Schlüssel auf ihrer Seite nutzen.

Ein Parameter in der Konfiguration jeder WAN-Verbindungen im SMGW **MUSS** festlegen, ob die Transport/TLS Verbindung (im Rahmen der Festlegungen des Schutzprofiles [GW_PP]) dauerhaft oder nur für eine Transaktion geöffnet bleibt.

3.2.5 Wake-Up Service

Dieser Abschnitt beschreibt den Wake-Up Service, der von einem SMGW umzusetzen ist.

3.2.5.1 Beschreibung des Anwendungsfalls

Über einen Wake-Up Service **MUSS** der SMGW Administrator den Aufbau eines TLS-Kanals für das Kommunikationsszenario MANAGEMENT anfordern können. Der SMGW Administrator **DARF** den Wake-Up Service deaktivieren, falls dieser nicht benötigt wird. Eine anschließende erneute Aktivierung des Wake-Up Service **MUSS** möglich sein.

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

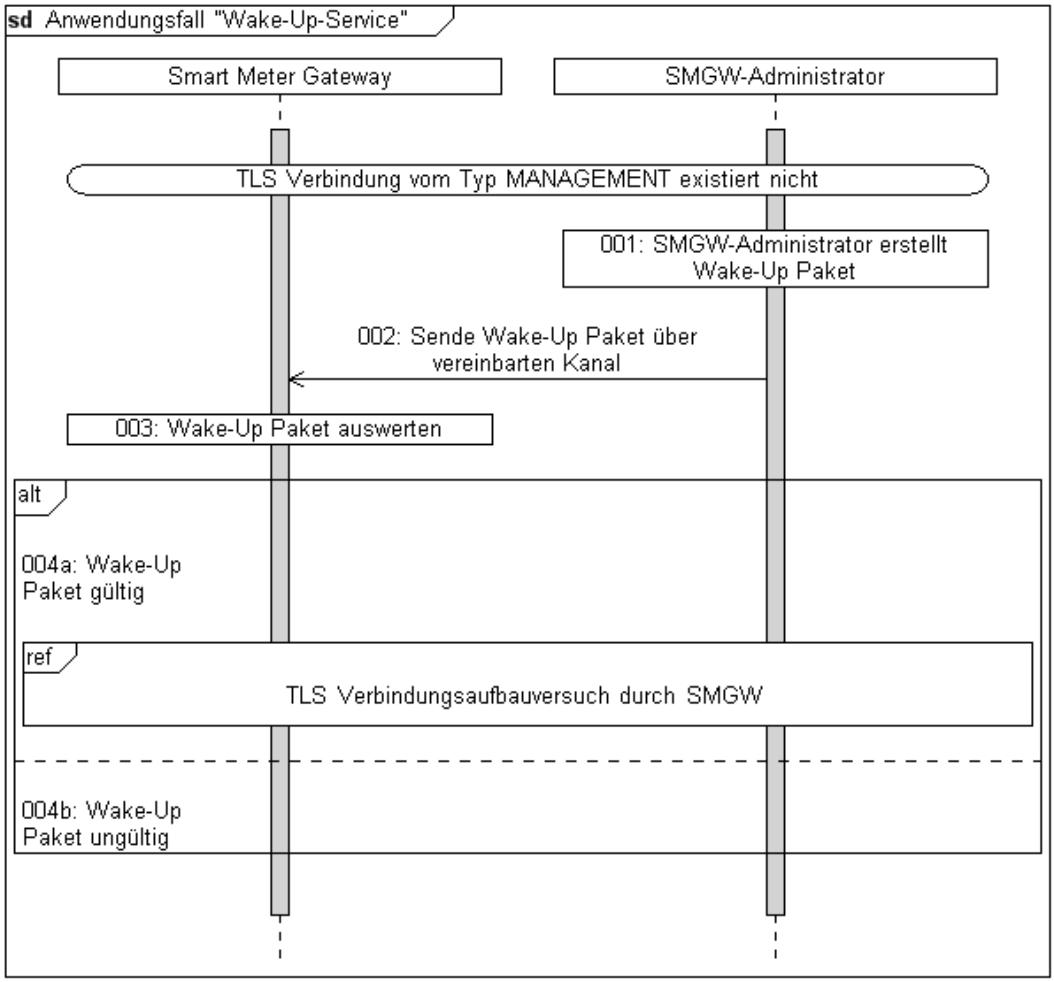

Abbildung 8: Sequenzdiagramm für den Anwendungsfall „Wake-Up Service“

Step	Event	Process/Activity	Info Producer	Info Receiver	Data Exchanged
001	SMGW Administrator benötigt einen „MANAGEMENT“ Kanal zum SMGW	SMGW Administrator erstellt ein Wake-Up Paket für das SMGW			
002		SMGW Administrator sendet Wake-Up Paket	SMGW Administrator	SMGW	Wake-Up Paket
003	SMGW hat Wake-Up Paket empfangen	SMGW-wertet Wake-Up Paket aus			
004a	Wake-Up Paket ist gültig	SMGW startet den TLS Verbindungsaufbau zum SMGW Administrator			
004b	Wake-Up Paket ist ungültig	Keine weitere Aktion des SMGW			

Tabelle 7: Beschreibung Anwendungsfall „Wake-Up Service“

3.2.5.2 Datenstruktur des Wake-Up Pakets

Der Aufbau des Wake-Up Pakets, das der SMGW Administrator sendet, **MUSS** den Festlegungen in „Anhang A: Datenstruktur Wake-Up Paket“ entsprechen.

3.2.5.3 Anforderungen an den Transportweg des Wake-Up Pakets

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 der TLS-Kanal aufgebaut wird.

3.2.5.4 Verarbeitung eines Wake-Up Pakets

Die folgenden Verarbeitungsregeln gelten für das SMGW:

1. Bei Empfang eines (potentiellen) Wake-Up Pakets **MUSS** (in dieser Reihenfolge) geprüft werden ob,
   a. die Kennzeichnung des Wake-Up Pakets übereinstimmt.
      Damit das SMGW nicht bei jedem empfangenem Paket eine vollständige Wake-Up Paket Prüfung vornimmt, sind zuerst die ersten drei Bytes des Pakets (Header+Version) zu überprüfen. Diese **MÜSSEN** der Zeichenkette „WU“ und der aktuelle Version (01h) entsprechen.
   b. das SMGW Adressat dieses Paketes ist.
      Dazu wird die im Paket enthaltene Geräteidentifizierung mit den Identifikationsdaten des SMGW verglichen. Die beiden Werte **MÜSSEN** übereinstimmen.
   c. die Nachricht in einem akzeptablen Zeitrahmen versendet/empfangen worden ist.
      Dazu ist im Wake-Up Paket ein Zeitstempel enthalten. Das SMGW **MUSS** prüfen,

ob der übertragene Zeitstempel mehr als **30** Sekunden von der aktuellen Systemzeit im SMGW abweicht. Ist dies der Fall, so **DARF** Wake-Up Paket vom SMGW **NICHT** akzeptiert werden. Dies soll das Wiederverwenden des Paketes zu einem beliebigen Zeitpunkt verhindern.

d. das Wake-Up Paket noch nicht empfangen wurde.

e. die Signatur des Pakets vom SMGW Administrator stammt.
Die Dienste des Sicherheitsmoduls werden dabei für die Signaturprüfung verwendet. Um DoS-Attacken gegen das SMGW zu erschweren **MUSS** das SMGW die Anzahl der Wake-Up Paket Signaturprüfungen innerhalb eines Zeitraumes einschränken.

2. Konnten Teile des Inhaltes einer Nachricht nicht verifiziert werden, d.h. die Überprüfung der Kennzeichnung, der Geräteidentifizierung, des Zeitstempels oder der Signatur sind fehlerhaft, so wird der weitere Prüfungsvorgang beim ersten Fehler unterbrochen und die Nachricht sofort verworfen. Auf der Applikationsschicht **DARF KEIN** Feedback zum Teilnehmer im WAN zurückgesendet werden. Der entsprechende Prozess wird terminiert.
3. Konnte der Inhalt der Nachricht verifiziert werden, so wird die Nachricht auch jetzt verworfen. Es **DARF KEIN** Feedback zum Sender zurückgeschickt werden. Vom SMGW **MUSS** jedoch ein TLS-Kanal zum SMGW Administrator im WAN initiiert werden, sofern dieser TLS-Kanal nicht schon aufgebaut ist. Die entsprechenden Adressierungsdaten **MÜSSEN** im SMGW vorkonfiguriert sein. Das SMGW **MUSS** sich das letzte akzeptierte Wake-Up Paket (bzw. einen Hash über dieses Paket) merken und **DARF** bei wiederholten Empfang desselben Paketes **NICHT** erneut einen TLS-Kanal aufbauen (siehe Schritt 1d).

Der Wake-Up Service **MUSS** als Teilprozess im SMGW so implementiert sein, dass dessen Ausführungspriorität niedriger ist als die der regulären Prozesse zur Messdatenverarbeitung. Der wiederholte Aufruf des Dienstes (z.B. als „denial of service“ Attacke) **DARF NICHT** die normalen Dienstleistungen des SMGW vollständig blockieren.

3.2.6 Zeitsynchronisation

3.2.6.1 Einleitung

Das SMGW **MUSS** in regelmäßigen Abständen seine lokale Uhrzeit mit einer vertrauenswürdigen Quelle abgleichen. Hierzu **MUSS** auf dem SMGW sichergestellt werden, dass die Zeitabweichung (ZA) der SMGW-Systemzeit von UTC und die "Round Trip Time" (RTT) der Synchronisationspakete jeweils festgelegte Schwellwerte nicht überschreiten. Dieses Kapitel enthält die dazu notwendigen Vorgaben.

Im Folgenden wird die maximal erlaubte Zeitabweichung ZA_{max} und die maximal erlaubte RTT RTT_{max} genannt.

Hinweis: Zukünftig ist der Umstieg auf ein effizienteres Verfahren mit vergleichbarem Sicherheitsniveau zur Zeitsynchronisation geplant, das sich noch zwischen BSI und PTB in Vorbereitung befindet.

3.2.6.2 Einsatzumgebung

Das SMGW synchronisiert ausschließlich mit einem oder mehreren Zeitservern des SMGW-Admin (siehe Kapitel 3.2.6.3), die wiederum mit den Zeitservern der PTB synchronisieren. Für eine korrekte Fehlerbetrachtung im Rahmen dieser Einsatzumgebung müsste das Fehlerkontingent der Strecke SMGW ←→ SMGW Admin als auch das der Strecke SMGW Admin ←→ PTB betrachtet werden. Da die Latenzzeiten zwischen SMGW Admin und PTB aber auf Grund der Netzinfrastruktur deutlich geringer als zwischen SMGW Admin und SMGW sind, wird davon ausgegangen, dass der gesamte Fehler durch die Strecker SMGW ←→ SMGW Admin dominiert wird. Damit wird im Folgenden für die Betrachtung des möglichen Fehlers nur die Strecke zwischen SMGW und SMGW Admin betrachtet.

3.2.6.3 Zeitsynchronisation zwischen SMGW und SMGW Administrator

Das SMGW **MUSS** über eine RTC (Real Time Clock) verfügen und **MUSS** seine lokale Uhrzeit mit einer vertrauenswürdigen, externen Zeitquelle, die vom SMGW Administrator bereitgestellt wird, synchronisieren.

Zusätzlich **MUSS** das SMGW über eine RTC (Real Time Clock) verfügen. Die RTC **MUSS** durch die Systemzeit des Betriebssystems gestellt werden. Nach einem Spannungsausfall **KANN** die Betriebssystemzeit von der RTC gestellt werden, sofern die Abweichung der RTC noch unterhalb der Warnschwelle (siehe Kapitel 3.2.6.3.2) liegt, ansonsten **MUSS** eine Zeitsynchronisation mit dem NTP-Server durchgeführt werden.

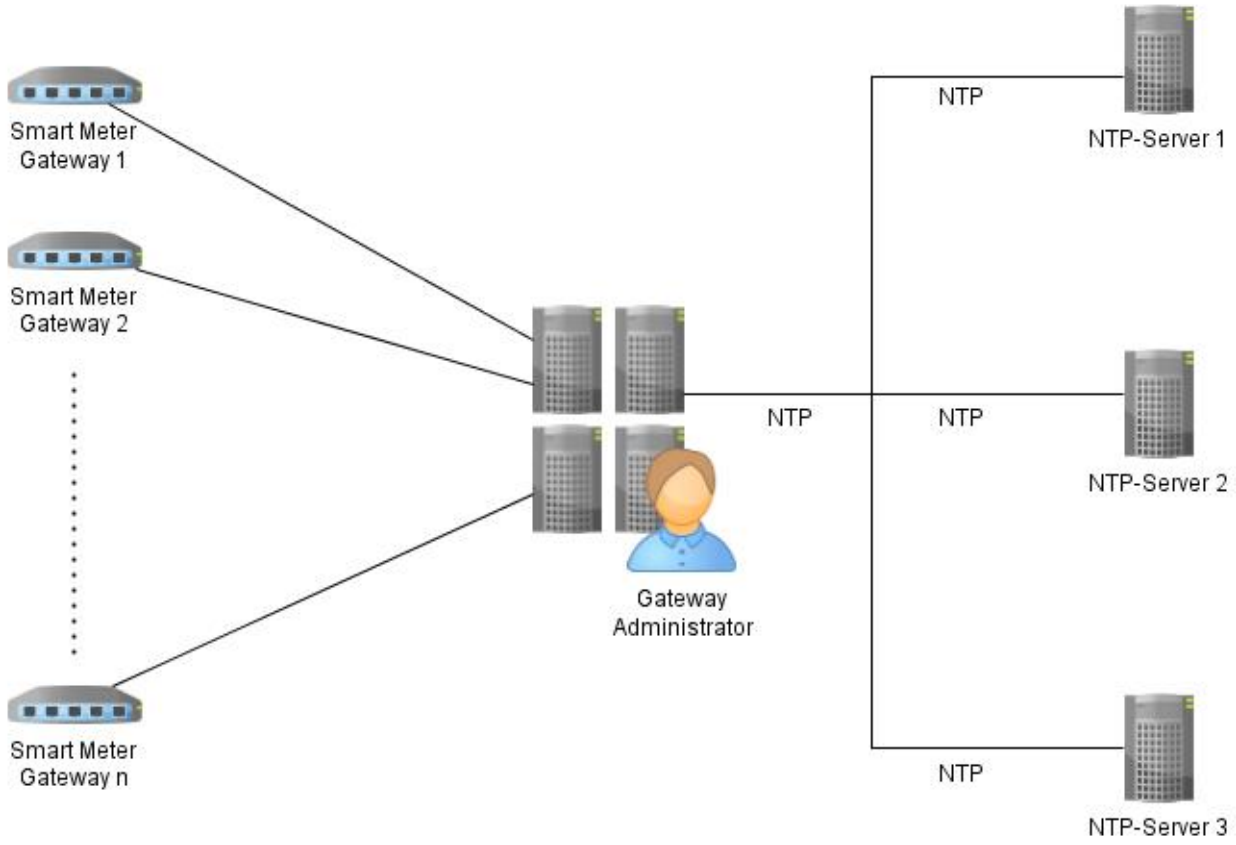

Abbildung 9: Zeitsynchronisation zwischen SMGW und SMGW Administrator

Die Geräteuhr **MUSS** so synchronisiert werden, dass die Abweichung zur gesetzlichen Zeit stets weniger als 3% der kleinsten Messperiode[4] beträgt.

Das SMGW **MUSS** mindestens eine Auflösung von 5 Minuten als kleinste Messperiode unterstützen. Ein SMGW **DARF** kürzere abrechnungsrelevante Zeiträume (unter 5 Minuten) unterstützen, sofern sichergestellt wird, dass die Abweichung zur gesetzlichen Zeit stets weniger als 3% der Messperiode beträgt.

Im Falle einer größeren Abweichung **MUSS** ein Eintrag in das Eichlog erfolgen und das SMGW **MUSS** den SMGW-Admin informieren. Weitere eingehende Messwerte **MÜSSEN** danach entsprechend gekennzeichnet werden (siehe Kapitel 4).

Beispiel: Soll ein SMGW Tarifmodelle verarbeiten können, die eine Auflösung von 5 Minuten vorsehen, beträgt die maximal zulässige Abweichung 9 Sekunden. Bei einer Abweichung über 9 Sekunden informiert das SMGW den SMGW-Admin und weitere eingehende Messwerte werden danach entsprechend gekennzeichnet.

[4] Die kleinste Messperiode ist als der kleinste, abrechnungsrelevante Zeitraum zu verstehen, der in der Messwerterfassung und in den Auswertungsprofilen verwendet wird.

Die Nutzung von anderen Technologien (wie DCF77) zur Zeitsynchronisation ist nicht zulässig.

3.2.6.3.1 Re-Synchronisierung der lokalen Zeit

Eine Re-Synchronisation der lokalen Zeit **MUSS** in Anlehnung an [RFC5905] erfolgen.

3.2.6.3.2 Vermeidung von Fehl-Synchronisierungen

Die Round-Trip-Time (RTT) bzw. die Gesamtverzögerung ist i.d.R. für die Genauigkeit der Synchronisation unerheblich, solange gewährleistet ist, dass die Verzögerungen auf dem Hin- und Rückweg vom NTP-Server ungefähr gleich sind. Zur Vermeidung von Fehl-Synchronisationen **MUSS** jedoch folgender Punkt beachtet werden:

Das SMGW muss bei jeder durchgeführten Zeitmessung die Einhaltung von zwei Bedingungen überprüfen:

1. $RTT < RTT_{max}$ mit $RTT_{max} < ZA_{max}$
2. $|ZA| + 0{,}5 * RTT < ZA_{max}$ (siehe [5])

Durch die erste Bedingung werden Messungen mit zu langer RTT verworfen, um den Einfluss einer Delay-Attacke zu minimieren.

Die zweite Bedingung stellt sicher, dass die Uhrzeit des SMGW innerhalb der erlaubten Toleranz verbleibt.

Die Festlegung von ZA_{max} wird durch das kleinste gewünschte Abrechnungsintervall beeinflusst. Es kann jedoch nicht beliebig gewählt werden, da eine untere Schranke für RTT_{max} maßgeblich durch die Übertragungstechnik bestimmt wird.

Beispiel:

In dem obigen Beispiel (ZA_{max} < 9 Sekunden) darf eine Synchronisierung nur dann als gültig akzeptiert werden, wenn |ZA|+0,5*RTT maximal 9 Sekunden nicht überschreitet. Der SMGW-Admin wird durch einen Eintrag im Logfile unterrichtet, wenn die RTT den vorgegebenen Zeitraum nicht einhalten konnte und deshalb keine Synchronisierung durchgeführt werden konnte.

Ist eine korrekte Synchronisierung über eine Zeit T nicht möglich wird der SMGW-Admin alarmiert und es erfolgt ein Eintrag in das Eich-Log. Diese Zeit T berechnet sich aus

$$T = \text{Warnschwelle} * \text{kleinste\_Messperiodendauer} * \text{eichrechtlich\_erlaubte\_Toleranz} / \text{Max\_SMGW\_Zeitdrift}$$

[5] ZA bezieht sich auf die Systemzeit des Betriebssystems, bereitgestellt durch den ntp Dienst. Diese Bedingung muss im Wirkbetrieb eingehalten werden. Im Störungsfall oder nach einer vorübergehenden Außerbetriebnahme kann die Prüfung dieser Bedingung entfallen.

Beispiel:

$$T = 80\% * 15 \text{ Minuten} * 3\% / 50 \text{ ppm}$$
$$= 0{,}80 * 900 \text{ s} * 0{,}03 / 0{,}00005$$
$$= 432000 \text{ s} (=5 \text{ Tage})$$

3.2.6.3.3 Technische Umsetzung

Das SMGW **MUSS** die in den folgenden zwei Kapiteln (3.2.6.3.3.1 und 3.2.6.3.3.2) beschriebenen Kommunikationsszenarien unterstützen, wobei der SMGW-Admin die Wahlfreiheit hat, welches der beiden Verfahren eingesetzt wird.

3.2.6.3.3.1 Zeitsynchronisation über einen Webservice (ntp-over-http)

Die Zeitsynchronisierung erfolgt in diesem Kommunikationsszenario über einen vom SMGW Admin bereitgestellten Web-Service[6].

Die Kommunikation mit dem Webservice **MUSS** über einen TLS 1.2 gesicherten Kanal erfolgen. Als Transportprotokoll wird HTTP eingesetzt. Die NTP-Nutzinformationen (nach [RFC5905]) werden im HTTP Body übertragen. Unnötige Informationen im HTTP Header **MÜSSEN** vermieden werden, um unnötige Verzögerungen bei der Übertragung zu vermeiden. Die Gesamtgröße der übertragenen Pakete (HTTP Header und HTTP Body mit NTP-Nutzinformationen) **MÜSSEN** 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[7].

3.2.6.3.3.2 Zeitsynchronisation über einen gesicherten Kanal (ntp-over-TLS)

Die Zeitsynchronisierung erfolgt in diesem Kommunikationsszenario mit einem vom SMGW Admin bereitgestellten NTP-Service.

Die Kommunikation mit dem NTP-Service **MUSS** über einen TLS 1.2 gesicherten Kanal erfolgen. Über den gesicherten Kanal werden die NTP-Nutzinformationen (nach [RFC5905]) übertragen. Andere Informationen, als das NTP-Paket nach [RFC5905], **DÜRFEN NICHT** über diesen Kanal übertragen werden.

Es **MUSS** zunächst der TLS gesicherte Kanal aufgebaut werden, bevor die Zeitsynchronisation per NTP durchgeführt wird, d.h. die Zeit, die für den Kanalaufbau benötigt wird, **DARF** das NTP-Protokoll **NICHT** beeinflussen.

Es **MÜSSEN** mehrere Kommunikationsendpunkte per Kommunikationsprofil konfigurierbar sein. Ist ein Endpunkt nicht erreichbar und stehen alternative Endpunkte zur Verfügung, **MUSS** das SMGW einen alternativen Endpunkt zur Synchronisierung heranziehen.

[6] verwendet wird der Admin-Service Kanal ohne CMS

[7] Je nach Anbindung des SMGW, kann die Laufzeit auf dem Hin- und Rückkanal sehr stark schwanken. Um nicht weitere Verzögerungen aufgrund unterschiedlich großer Pakete zu erhalten, sollten diese in etwa dieselbe Größe aufweisen.

3.2.6.3.4 Sonderfälle

Wird ein SMGW erstmalig in Betrieb genommen, **MUSS** zunächst eine Zeitsynchronisierung durchgeführt werden. Da aufgrund der bisher nicht initialisierten Zeit keine Gültigkeitsprüfung der Zertifikate möglich ist **DARF** eine Gültigkeitsprüfung entfallen; ebenso **DARF** eine Prüfung der zweiten Bedingung aus Kapitel 3.2.6.3.2 entfallen.

Die Kommunikation nach einem erstmaligen Start **SOLLTE** randomisiert zeitverzögert durchgeführt werden.

Generell gilt, kann ein SMGW eine gültige Uhrzeit nicht (mehr) sicherstellen, **MUSS** eine Zeitsynchronisierung durchgeführt werden. Da aufgrund der ungültigen Zeit keine Gültigkeitsprüfung der Zertifikate möglich ist **DARF** die Gültigkeitsprüfung entfallen.

3.3 Vorgaben an die Kommunikationsverbindungen in das LMN

3.3.1 Übersicht

Dieses Kapitel (3.3.1) hat informativen Charakter.

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 Kapitel 3.3.2 skizziert. Die zur Realisierung dieser Anwendungsfälle notwendigen Kommunikationsszenarien werden in Kapitel 3.3.3 definiert.

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

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

3.3.2 Anwendungsfälle an der LMN Schnittstelle

Dieses Kapitel listet diejenigen Anwendungsfälle auf, die zwingend eine Kommunikation des SMGW mit Zählern im LMN erfordern. Das SMGW **MUSS** mindestens diese Anwendungsfälle unterstützen.

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

1. LMN Zählerverwaltung
2. Abruf/Empfang von Messwerten

LAF1: LMN Zählerverwaltung

Das SMGW **MUSS** die Konfiguration der Zähler im LMN unterstützen:

- Registrierung/Konfiguration

  Im SMGW **MÜSSEN** Zähler durch den SMGW Administrator registriert, konfiguriert und einem Letztverbraucher zugeordnet werden können.

- Schlüssel-/Zertifikatsmanagement

  Das SMGW **MUSS** auf Anforderung des SMGW Administrators Schlüssel und Zertifikate für die Kommunikation mit Zählern im LMN erstellen, verteilen, aktivieren, deaktivieren bzw. löschen können.

  Folgende Fälle **MÜSSEN** unterstützt werden:

  - Generieren von öffentlichen und privaten Schlüsseln für LMN Zähler
  - Generieren von selbst-signierten TLS Zertifikaten durch das SMGW
  - Einbringen und Erneuern der TLS Zertifikate für bidirektional angeschlossene Zähler (siehe „Anlage IVa: Feinspezifikation „Drahtgebundene LMN-Schnittstelle““ und „Anlage IIIb: Feinspezifikation „Drahtlose LMN-Schnittstelle“ Teil 2“)
  - Austausch des jeweiligen zählerindividuellen „Master“ Schlüssels für die symmetrische Verschlüsselung bei drahtlos, bidirektional angeschlossenen Zählern. Dazu muss ein TLS Kanal zum Zähler aufgebaut werden wie in „Anlage IIIb: Feinspezifikation „Drahtlose LMN-Schnittstelle“ Teil 2“ spezifiziert.

Dieser Anwendungsfall erfordert aufgrund des Request-Response Kommunikationsmusters eine bidirektionale Verbindung (siehe Kommunikationsszenario LKS1 in Kapitel 3.3.3).

LAF2: Abruf/Empfang von Messwerten

Das SMGW **MUSS** die in den Zählern gebildeten Messwerte abfragen bzw. periodisch zugelieferte Werte empfangen können. 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 ein Messwert zur Verfügung, wenn er dazu vom SMGW aufgefordert wird. Das SMGW **MUSS** Einzelabrufe von Messwerten sowohl bei Bedarf als auch periodisch durchführen können.

  Dieser Anwendungsfall erfordert aufgrund des Request-Response Kommunikationsmusters eine bidirektionale Verbindung (siehe Kommunikationsszenario LKS1 in Kapitel 3.3.3).

- Zulieferung von Messwerten

  Das SMGW **MUSS** eine periodische Zulieferung von Messwerten, die vom Zähler unaufgefordert gesendet werden, unterstützen.

Dieser Anwendungsfall erfordert mindestens eine unidirektionale Verbindung mit einem Zähler als Sender und dem SMGW als Empfänger (siehe Kommunikationsszenario LKS2 in Kapitel 3.3.3).

3.3.3 Kommunikationsszenarien

Die in Kapitel 3.3.2 skizzierten Anwendungsfälle an der LMN Schnittstelle lassen sich auf folgende Kommunikationsszenarien abbilden, die vom SMGW unterstützt werden **MÜSSEN**:

- 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 8: Kommunikationsszenarien an der LMN Schnittstelle

LKS1: BIDIREKTONAL

Das folgende Diagramm zeigt das Kommunikationsmuster bei bidirektionaler Zählerkommunikation.

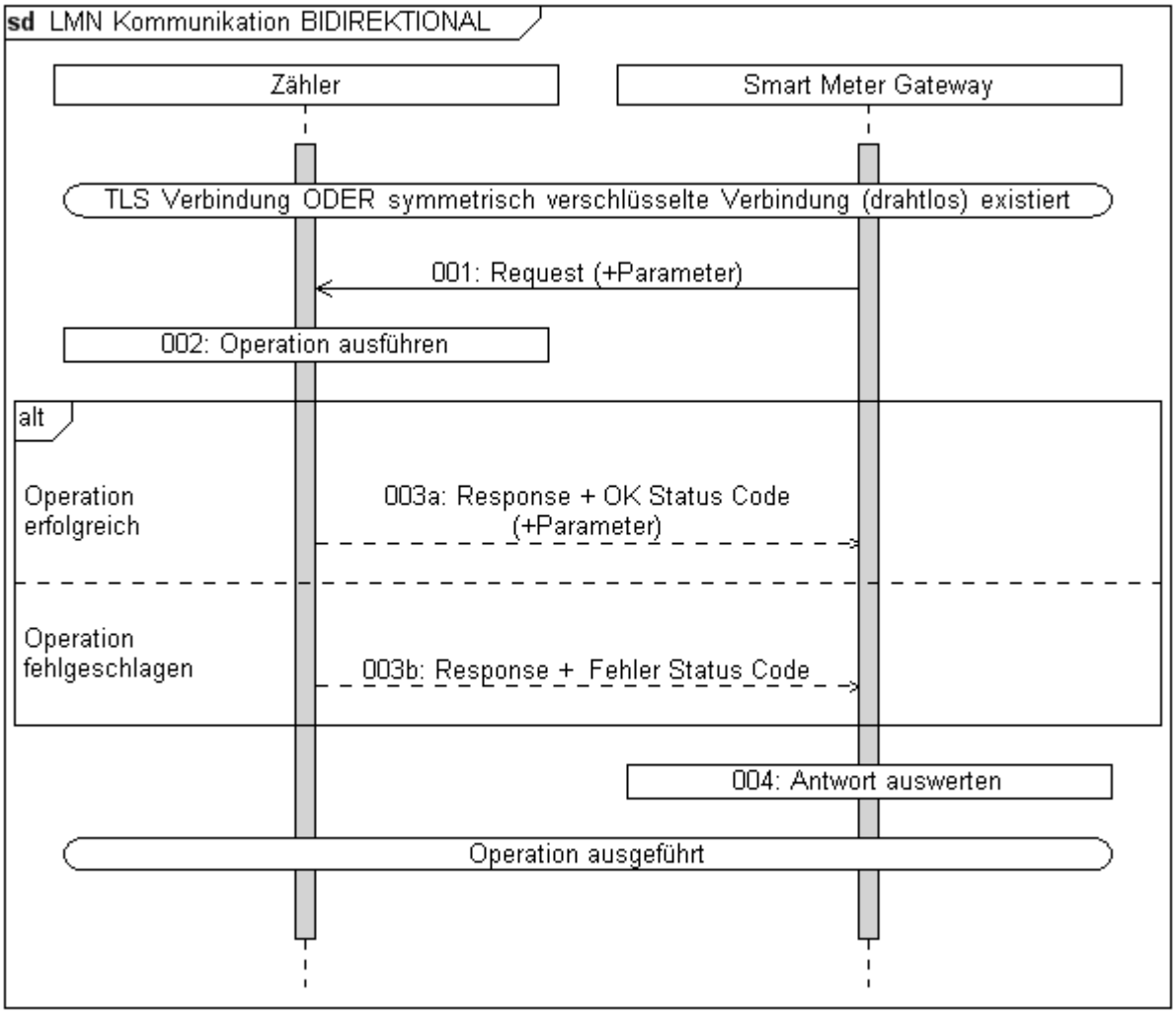

Abbildung 10: Sequenzdiagramm für bidirektionale LMN Kommunikation

Vorbedingung:

Es besteht eine TLS-Verbindung oder bei drahtlos angebundenen Zählern eine mit symmetrischer Kryptographie gesicherte Verbindung zwischen Zähler und SMGW.

Rolle des Smart Meter Gateways:

Client

Step	Event	Process/Activity	Info Producer	Info Receiver	Data Exchanged.
001		SMGW erstellt und sendet Anfrage	SMGW	Zähler	Request (+Parameter)
002	Zähler führt die gewünschte Operation aus, z.B. ermittelt die angefragten	Zähler führt Anfrage aus			

	Messwerte				
003a	Operation erfolg-reich beendet	Zähler sendet Response an SMGW	Zähler	SMGW	Response-Code OK (+Parameter)
003b	Operation nicht erfolgreich beendet	Zähler sendet Response an SMGW	Zähler	SMGW	Response mit Fehler Code
004	SMGW empfängt Zählerantwort	SMGW verarbeitet Antwort			

Tabelle 9: Beschreibung Kommunikationsszenario LMN bidirektional

LKS2: UNIDIREKTIONAL

Das folgende Diagramm zeigt das Kommunikationsmuster bei unidirektionaler Zählerkommunikation.

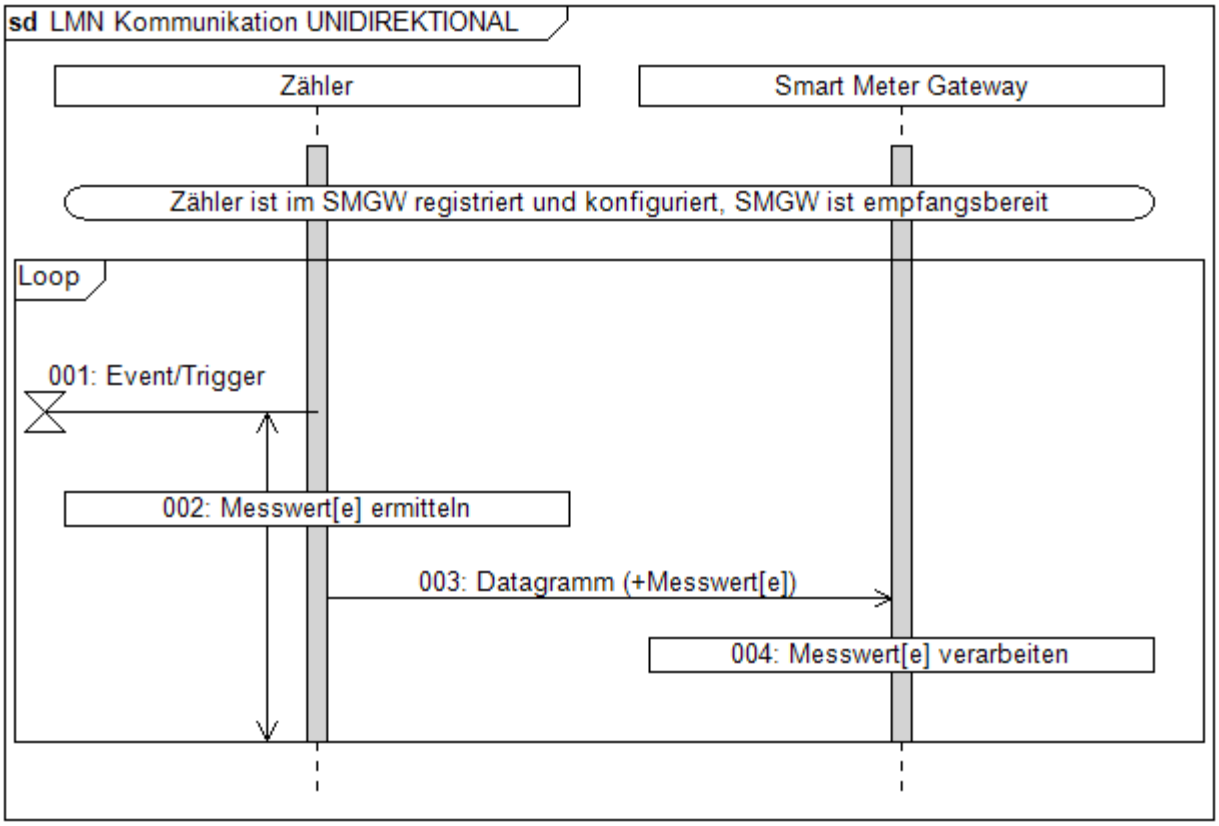

Abbildung 11: Sequenzdiagramm für unidirektionale LMN Kommunikation

Vorbedingung:

Der Zähler, der unidirektional Datagramme an das SMGW sendet, ist im SMGW registriert und konfiguriert.

Rolle des Smart Meter Gateways:

Receiver

Step	Event	Process/Activity	Info Producer	Info Receiver	Data Exchanged.
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
004	SMGW empfängt Messwerte	SMGW verarbeitet Messwerte			

Tabelle 10: Beschreibung Kommunikationsszenario 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 vor Abhören, Manipulation und Fälschung geschützt werden. Das SMGW **MUSS** dabei Sicherungen für uni- und bidirektionale Kommunikation unterstützen, wie in den folgenden Unterkapiteln dargestellt.

3.3.4.1 Sicherung der LMN Kommunikation mit TLS

Das SMGW **MUSS** TLS gemäß [BSI TR-03109-3] implementieren. Hierbei **MUSS** das SMGW sowohl die Rolle des TLS-Servers als auch die Rolle des TLS-Clients übernehmen können. Das SMGW **MUSS** sein Sicherheitsmodul während des TLS-Handshakes analog zu den in Kapitel 5.1.1 dargestellten kryptographischen Operationen verwenden.

Zur gegenseitigen Authentifizierung zwischen SMGW und Zählern im LMN **MÜSSEN** LMN-Zertifikate verwendet werden. Es werden grundsätzlich X.509-Zertifikate eingesetzt. Die Zertifikate sind selbst-signiert. Die LMN-Zertifikate (SMGW und Zähler) stammen somit nicht aus der in [BSI TR-03109-4] definierten SM-PKI. Details zum LMN Zertifikatsprofil sind in „Anhang B: Zertifikate im LMN“ definiert.

3.3.4.2 Sicherung der LMN Kommunikation mit symmetrischen Verfahren

Das SMGW **MUSS** für drahtlos kommunizierende Zähler ein symmetrisches kryptographisches Verfahren bereitstellen. Dazu **MUSS** das SMGW die kryptographischen Algorithmen implementieren, die für die symmetrische Zählerdatensicherung in [BSI TR-03109-3] gefordert werden.

3.3.5 Kommunikationsprotokolle

In diesem Abschnitt werden die Anforderungen an das SMGW in Bezug auf die zu unterstützenden Kommunikationsprotokolle im LMN festgelegt. Prinzipiell wird hier unterschieden zwischen Anforderungen, die auf die Unterstützung von Applikationsdatenformaten abzielen, und Anforderungen an das Schnittstellenprotokoll für den Transport der Applikationsdaten.

Das SMGW **MUSS** gemäß [GW_PP] externe Schnittstellen für den Anschluss von Zählern im LMN bereitstellen. Werden diese Schnittstellen nicht genutzt, **MÜSSEN** sie durch den SMGW Administrator deaktiviert werden können.

Die folgende Abbildung 12 zeigt die Gesamtheit der LMN Protokollstapel im SMGW. Die Protokollstapel haben abhängig von der physikalischen Ebene unterschiedliche Ausprägungen, die in den nächsten Abschnitten detailliert werden.

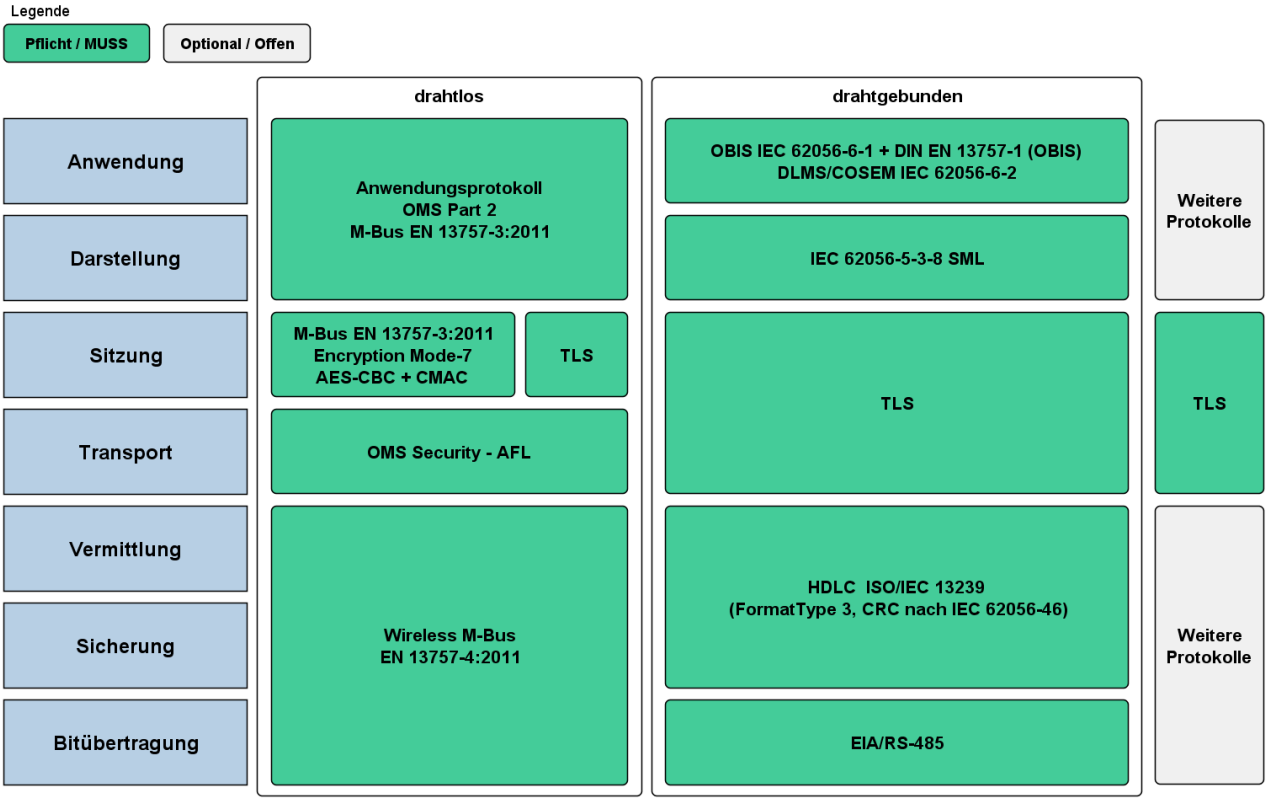

Abbildung 12: Protokollstapel im LMN (für drahtlose und drahtgebundene Kommunikation)

3.3.5.1 Anwendungsprotokolle

Das SMGW **MUSS** die folgenden Anwendungsprotokolle unterstützen:

- [EN 13757-3] M-Bus DIN EN 13757-3: Kommunikationssysteme für Zähler und deren Fernablesung Teil 3: Spezielle Anwendungsschicht, gemäß „Anlage IIIa: Feinspezifikation „Drahtlose LMN-Schnittstelle“ Teil 1“ mit folgenden Einschränkungen:

OSI-Layer	**Verbindliche Kapitel der Anlage IIIa: Feinspezifikation „Drahtlose LMN-Schnittstelle“ Teil 1**
Physical Layer	„2.2 Wireless Communication (wM-Bus)“ zusammen mit Annex L und Annex I.
Data Link Layer	„3.2 Wireless Communication (wM-Bus)“
Application Layer - Allgemein	“4.2 Common Part for all Application Layers”[a] (ohne Abschnitt “4.2.5 Encryption”[b]) “4.3.2 Application Errors after Command”
Application Layer - Protokoll	„5.1 M-Bus Application Protocol“ zusammen mit Annex A, Annex B, Annex E, Annex G1 und G2.
[a] Unterbrecher und Regler (CLS) **DÜRFEN NICHT** über die Schnittstelle IF_GW_MTR des SMGW kommunizieren. [b] Verschlüsselung und Authentifikation **MUSS** gemäß Anlage IIIb: Feinspezifikation „Drahtlose LMN-Schnittstelle“ Teil 2 implementiert werden.	

- [IEC 62056-6-1] Object Identification System (OBIS),
- [EN 13757-1] M-Bus DIN EN 13757-1: Kommunikationssysteme für Zähler und deren Fernablesung Teil 1: Datenaustausch (nur OBIS Kennzahlen),
- [IEC 62056-6-2] COSEM Interface classes.

Das SMGW **KANN** weitere Anwendungsprotokolle und Datenformate unterstützen. Die Übertragung der Daten **MUSS** über einen sicheren Transportkanal, wie in Kapitel 3.3.4 beschrieben, erfolgen.

3.3.5.2 Transferprotokolle und Transportsicherung

Das SMGW **MUSS** die folgenden Transferprotokolle unterstützen:

- [IEC 62056-5-3-8] Smart Message Language (SML),

- TLS (gemäß den Vorgaben in [BSI-TR-03109-3]),
- OMS Authentication and Fragmentation Layer (AFL), siehe "Anlage IIIb: Feinspezifikation „Drahtlose LMN-Schnittstelle" Teil 2".

Die aktuell standardisierte M-Bus Verschlüsselung in [EN 13757-3] ist nicht ausreichend und wurde daher erweitert. Für die technische Umsetzung dieser erweiterten Kryptoverfahren wurde ein neuer „Authentication and Fragmentation Layer (AFL)" spezifiziert. Dieser AFL-Layer **MUSS** mit „M-Bus Encryption-Mode-7" implementiert werden.

Das SMGW **MUSS** im LMN mindestens eine drahtlose und eine drahtgebundene Schnittstelle zur Verfügung stellen. Diese werden in den folgenden Abschnitten detailliert.

3.3.5.2.1 Drahtlose Schnittstelle

Das SMGW **MUSS** eine Funkschnittstelle zum drahtlosen Anschluss von Zählern besitzen. Das auf der Funkschnittstelle realisierte Übertragungsprotokoll **MUSS** konform sein zur Norm [EN 13757-4] „M-Bus DIN EN 13757-4, Kommunikationssysteme für Zähler und deren Fernablesung Teil 4: Zählerauslesung über Funk, Fernablesung von Zählern im SRD-Band von 868 MHz bis 870 MHz" - im Folgenden kurz wM-Bus genannt.

Das SMGW **MUSS** Zähler unterstützen, welche gemäß der wM-Bus Spezifikation [EN 13757-4] in folgenden Betriebsarten arbeiten können:

Betriebsart	***Kommunikation***	***m/o***[8]	***Beschreibung***
S1	unidirektional	m	Der Zähler überträgt einige Male je Tag zu einem ortsfesten Empfangspunkt.
S2	bidirektional	m	Der Zähler ist mit einem Empfänger ausgestattet, der ständig bereit ist oder synchronisiert arbeitet, ohne erweiterte Vorbereitung für das Wecken.
T1	unidirektional	m	Der Zähler überträgt nur in kurzen Datenblöcken in kurzen Zeitabständen.
T2	bidirektional	m	Der Zähler übermittelt regelmäßig wie in Betriebsart T1 und sein Empfänger wird nach dem Ende jeder Übertragung für eine kurze Dauer eingeschaltet und rastet ein, wenn er eine Rückmeldung erhält.

Tabelle 11: Betriebsarten für wM-Bus

Falls nur ein RF-Transceiver im SMGW verbaut ist, **MUSS** dieser konfigurierbar in den Modi S1/S2 oder T1/T2 arbeiten können bzw. die Modi in einem Wechselbetrieb bereitstellen.

[8] m = muss, o = optional

Es **MUSS** die wM-Bus Sicherungs- und Vermittlungsschicht gemäß [EN 13757-4] „M-Bus DIN EN 13757-4“ verwendet werden.

Das SMGW KANN weitere Funkprotokolle und/oder wM-Bus Modi implementieren, sie **MÜSSEN** dann den kryptographischen Anforderungen aus Kapitel 3.3.4 genügen.

3.3.5.2.2 Drahtgebundene Schnittstelle

Das SMGW **MUSS** eine Schnittstelle zum drahtgebundenen Anschluss von Zählern besitzen. Diese Schnittstelle **MUSS** als [EIA RS-485]-Schnittstelle realisiert werden.

Auf der Sicherungs- und Vermittlungsschicht **MÜSSEN** folgende Protokolle verwendet werden:

- High-Level Data Link Control (HDLC) FormatType 3 gemäß [IEC/ISO 13239:2002],
- Die Cyclic Redundancy Check (CRC) Berechnung für Header Check Sequence (HCS) und Frame Check Sequence (FCS) im HDLC Protokoll **MUSS** gemäß der Definition in [IEC 62056-46] erfolgen.
- Anlage IVa: Feinspezifikation „Drahtgebundene LMN-Schnittstelle“ spezifiziert, wie eine eindeutige und automatische Vergabe der HDLC Adressen der Zähler im LMN erreicht werden kann. Zusätzlich sind Methoden definiert zur Erkennung von bereits registrierten oder verstummten (entfernter) LMN-Busteilnehmer.

3.4 Vorgaben an die Kommunikationsverbindungen in das HAN

3.4.1 Übersicht

Dieses Kapitel (3.4.1) hat informativen Charakter.

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 Kapitel 3.4.2 skizziert. Zur Realisierung dieser Anwendungsfälle werden mehrere Kommunikationsszenarien herangezogen, welche vom SMGW unterstützt werden müssen. Diese werden in Kapitel 3.4.3 definiert. Die Anforderungen an die Sicherung der Kommunikationsverbindungen werden in Kapitel 3.4.4 formuliert. In Kapitel 3.4.5 werden die technischen Anforderungen an die HAN Schnittstelle dargelegt, während Kapitel 3.4.6 die notwendigen Parameter zur Kommunikation beschreibt.

3.4.2 Anwendungsfälle an der HAN Schnittstelle

Dieses Kapitel listet diejenigen Anwendungsfälle auf (gekennzeichnet mit dem Kürzel HAF*), die eine Kommunikation des SMGW mit Teilnehmern im HAN erfordern. Zusätzlich werden in diesem Kapitel die Anwendungsfälle beschrieben, die einen transparenten Kanal durch das SMGW zwischen CLS im HAN und EMT im WAN erfordern. Das SMGW **MUSS** mindestens diese Anwendungsfälle unterstützen.

Folgende Anwendungsfälle an der HAN-Schnittstelle werden definiert:

HAF1: Bereitstellung von Daten für den Letztverbraucher

HAF2: Bereitstellung von Daten für den Service-Techniker

HAF3: Transparenter Kommunikationskanal zwischen CLS und EMT

3.4.2.1 Anwendungsfall HAF1: Bereitstellung von Daten für den Letztverbraucher

Beschreibung

Das SMGW bietet eine Visualisierungsmöglichkeit über die Schnittstelle IF_GW_CON im HAN an, um dem Letztverbraucher Einsicht in seine Verbrauchsdaten und andere für den Letztverbraucher relevante Informationen zu ermöglichen.

Unter Verwendung des Anwendungsfalls HAF1 kann somit die Bereitstellung von abrechnungsrelevanten Daten und von aktuellen Messwerten sowie die zugehörigen Tarifinformationen gemäß den Anwendungsfällen der Tarifierung aus Kapitel 4 gewährleistet werden. Ebenso ermöglicht der Anwendungsfall HAF1 die Bereitstellung von historischen Daten gemäß Energieeffizienzrichtlinie [EER].

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

Für den jeweiligen Letztverbraucher zur Verfügung zu stellende Daten

Das SMGW **MUSS** mindestens folgende Informationen an der Schnittstelle für Anzeigeeinheiten bereitstellen:

- Datum und Systemzeit des SMGW
- Aktuelle Zählerstände in kWh oder m^3 der am SMGW angeschlossenen und dem Letztverbraucher zugeordneten Zähler.
- Aktuelle Tarifstufe je Auswertungsprofil.
- Historische Daten gemäß Energieeffizienzrichtlinie [EER]

  Dabei müssen Verbrauchs- sowie Einspeisewerte für die folgenden Zeiträume bereitgestellt werden:
  - die letzten 7 Tage, Tag für Tag
  - die letzte Woche (aggregiert)
  - das letzte Jahr (aggregiert)
  - mindestens die letzten 15 Monate (Monat für Monat aggregiert)
- Messwerte der letzten 24h in einer Granularität, wie sie das SMGW vom Zähler erfasst und zur Aktualisierung der abgeleiteten Register verwendet.

- Alle Daten des Letztverbraucher-Logs gemäß Kapitel 5.3.2.

Dieser Anwendungsfall kann unter Verwendung der Kommunikationsszenarien HKS1 und HKS2 umgesetzt werden.

Anmerkung: Damit eine Anzeigeeinheit eine konkrete Datenabfrage letztverbraucherspezifischer Daten erstellen kann, **MUSS** das SMGW die für einen Letztverbraucher verfügbaren Datenstrukturen auflisten können. Mittels dieser initialen Datenstrukturen kann die Anzeigeeinheit sukzessiv weitere Detailabfragen zu den verfügbaren Datenstrukturen stellen.

3.4.2.2 Anwendungsfall HAF2: Bereitstellung von Daten für den Service-Techniker

Beschreibung

Anwendungsfall HAF2 ermöglicht die Bereitstellung von Informationen aus dem Systemlog sowie weitere herstellerspezifische Diagnose-Informationen für den Service-Techniker über die Schnittstelle IF_GW_SRV.

Bereitzustellende Daten für den Service-Techniker

Das SMGW **MUSS** mindestens folgende Informationen für Service-Techniker an der Schnittstelle IF_GW_SRV im HAN bereitstellen:

- Alle Daten des Systemlogs

Weitere Diagnose-Informationen KÖNNEN angezeigt werden, wie zum Beispiel:

- Diagnose-Informationen
  - 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

Der Service-Techniker **DARF KEINE** personenbezogenen Daten abrufen können.

Dieser Anwendungsfall kann unter Verwendung der Kommunikationsszenarien HKS1 umgesetzt werden.

3.4.2.3 Anwendungsfall HAF3: Transparenter Kommunikationskanal zwischen CLS und EMT

Beschreibung

Der Anwendungsfall HAF3 ermöglicht es CLS im HAN über das SMGW mit autorisierten externen Marktteilnehmern im WAN zu kommunizieren. Das SMGW **MUSS** dafür eine Proxy-Funktionalität bereitstellen, um einen transparenten Kommunikationskanal bereitzustellen.

Für den Fall dass ein Kanal von einem EMT an ein CLS aufgebaut werden soll, **MUSS** die Initiierung indirekt über den SMGW-Admin erfolgen, da ein EMT keine direkte Verbindung zum SMGW aufbauen kann. Dazu sendet der SMGW-Admin einen entsprechenden Administrationsbefehl an das SMGW.

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

Dieser Anwendungsfall kann unter Verwendung der Kommunikationsszenarien HKS3 bis HKS5 umgesetzt werden.

3.4.3 Kommunikationsszenarien

Die in Kapitel 3.4.2 skizzierten Anwendungsfälle HAF1 bis HAF3 an der HAN Schnittstelle verwenden folgende fünf Kommunikationsszenarien (gekennzeichnet mit dem Kürzel HKS), die vom SMGW unterstützt werden **MÜSSEN:**

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

Die Kommunikationsszenarien HKS1 bis HKS5 unterscheiden sich in der Art und Weise der Authentifizierung des Teilnehmers im HAN (Letztverbraucher/Service-Techniker) sowie der Initiierung des transparenten Kommunikationskanals.

Im Folgenden werden diese Kommunikationsszenarien beschrieben.

3.4.3.1 Kommunikationsszenario HKS1: Bidirektionale Kommunikation im HAN bei Authentifizierung mittels HAN-Zertifikaten

In diesem Kommunikationsszenario erfolgt die Kommunikation zwischen dem SMGW und Teilnehmern im HAN bidirektional. In diesem Fall übernimmt das SMGW die TLS-Server-Rolle und der Teilnehmer im HAN die TLS-Client-Rolle.

Beim Aufbau der TLS-Verbindung zwischen dem Teilnehmer im HAN und dem SMGW wird im TLS-Handshake mittels der Zertifikate GW_HAN_TLS_CRT und CON_HAN_TLS_CRT und de-

ren zugehörigen Schlüsseln eine Client-Server Authentifizierung durchgeführt. Das Zertifikat CON_HAN_TLS_CRT ist dabei eindeutig einem dem SMGW bekannten Letztverbraucher oder Service-Techniker zugeordnet.

Akteur	*Beschreibung*
SMGW	Das SMGW agiert als TLS Server und verfügt über ein eindeutiges HAN-Zertifikat GW_HAN_TLS_CRT. Das Schlüsselmaterial zum HAN-Zertifikat ist im Sicherheitsmodul gespeichert.
Letztverbraucher/ Service-Techniker	Der Letztverbraucher/Servicetechniker agiert mithilfe von Anzeigeeinheiten/CLS als TLS Client und verwendet das HAN-Zertifikat CON_HAN_TLS_CRT zur Client Authentifizierung.

Tabelle 12: HKS1: Authentifizierung des Letztverbraucher/Service-Techniker mittels HAN-TLS-Client-Zertifikat

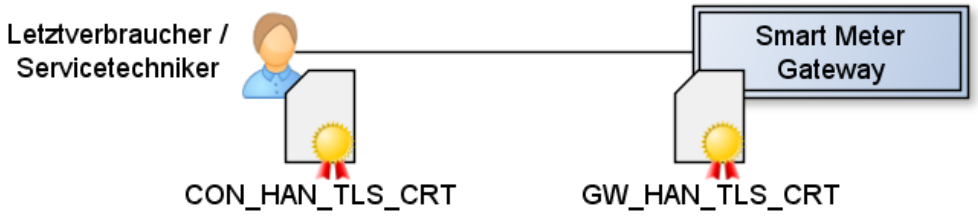

Abbildung 13: Authentifizierung des Letztverbrauchers/Service-Technikers mittels HAN-TLS-Client-Zertifikat

Nach erfolgreicher beidseitiger Authentifizierung **MUSS** das SMGW Ergebnisse zu den vom Letztverbraucher bzw. Service-Techniker abgesetzten Datenabfragen gemäß den Anwendungsfällen HAF1 bzw. HAF2 liefern. Es werden nur Daten übermittelt, die dem authentifizierten Letztverbraucher bzw. Service-Techniker zugeordnet sind.

3.4.3.2 Kommunikationsszenario HKS2: Bidirektionale Kommunikation im HAN bei Authentifizierung mittels eindeutiger Kennung und Passwort

In diesem Kommunikationsszenario erfolgt die Kommunikation zwischen dem SMGW und dem Letztverbraucher bidirektional. In diesem Fall übernimmt das SMGW die TLS-Server-Rolle und der Letztverbraucher nimmt mithilfe einer Anzeigeeinheit/CLS die TLS-Client-Rolle ein. Ein Service-Techniker **DARF** das Kommunikationsszenario HKS2 **NICHT** verwenden.

Beim Aufbau der TLS-Verbindung zwischen Letztverbraucher und dem SMGW wird im TLS-Handshake mittels des Zertifikats GW_HAN_TLS_CRT eine Server Authentifizierung durchgeführt. Anschließend werden mittels einer HTTP-Digest-Access-Authentication Kennung und Passwort abgefragt und an das SMGW übermittelt. Kennung und Passwort sind dabei eindeutig einem dem SMGW bekannten Letztverbraucher zugeordnet.

Akteur	*Beschreibung*
SMGW	Das SMGW fungiert als TLS Server und verfügt über ein eindeutiges HAN-Zertifikat GW_HAN_TLS_CRT. Das Schlüsselmaterial zum HAN-

Akteur	*Beschreibung*
	Zertifikat ist im Sicherheitsmodul gespeichert.
Anzeigeeinheit	Der Letztverbraucher agiert mithilfe von Anzeigeeinheiten/CLS als TLS Client und verwendet eine eindeutige Kennung und Passwort in einer HTTP-Digest-Access-Authentication. Das Passwort **MUSS** den Anforderungen aus [BSI-TR-03109-3] genügen.

Tabelle 13: HKS2: Authentifizierung des Letztverbrauchers mittels Kennung und Passwort

Abbildung 14: Authentifizierung des Letztverbrauchers mittels Kennung und Passwort

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

3.4.3.3 Kommunikationsszenario HKS3: Transparenter Kanal initiiert durch CLS

Beschreibung

Im Falle der Initiierung des transparenten Kanals durch das CLS **MUSS** das CLS SOCKSv5 [RFC1928] konforme Kommandos bei der initialen Kommunikation mit dem SMGW verwenden.

Beim Aufbau der TLS-Verbindung zwischen CLS und SMGW wird im SOCKS-TLS-Handshake mittels der Zertifikate GW_HAN_TLS_CRT und CLS_HAN_TLS_CRT und der zugehörigen Schlüssel eine Client-Server Authentifizierung durchgeführt. Das CLS-Zertifikat CLS_HAN_TLS_CRT ist dabei eindeutig einem dem SMGW bekannten CLS zugeordnet. Im SOCKS-Protokoll wird als Zieladresse ein eindeutiger Bezeichner für den EMT an das SMGW übermittelt. Das SMGW überprüft mittels der konfigurierten Proxy-Kommunikationsprofile die Zulässigkeit der Proxy-Verbindung und baut eine TLS Verbindung zum konfigurierten EMT auf. Dabei wird eine Client-Server Authentifizierung zwischen SMGW und dem EMT mittels der Zertifikate GW_WAN_TLS_CRT und EMT_WAN_TLS_CRT durchgeführt.

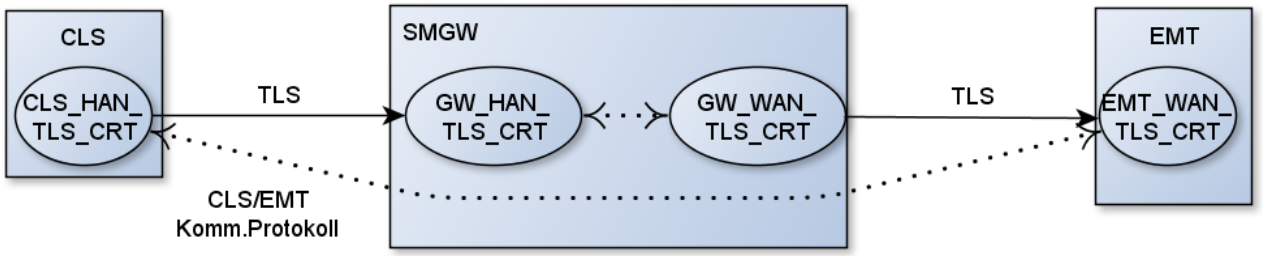

Abbildung 15: Transparenter Kanal initiiert durch CLS

CLS/EMT Adressierung

Beim Verbindungsaufbau muss der Initiator (das CLS) dem SMGW mitteilen, zu welchem Endpunkt dieser eine Verbindung aufnehmen möchte. Als Steuerungsprotokoll **MUSS** dazu SOCKSv5 [RFC1928] mit „TLS for SOCKSv5“ [DRAFT-IETF-AFT-SOCKS-SSL-00] eingesetzt werden.

Folgende Grafik zeigt den allgemeinen Protokollablauf bei SOCKSv5.

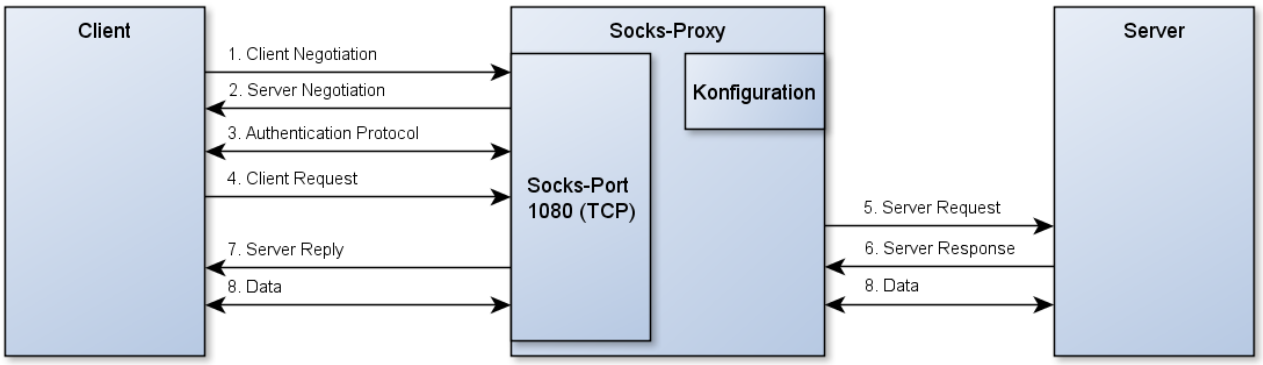

Abbildung 16: Protokollablauf SOCKSv5

Im SOCKSv5-ClientRequest wird zur Adressierung des EMT das Command „CONNECT“ mit einem Adresstype DomainName verwendet, welches den eindeutigen Bezeichner für den EMT als Endpunkt enthält. Dieser DomainName Bezeichner ist im Proxy-Kommunikationsprofil als „Adresse(n) des Kommunikationspartners im HAN“ hinterlegt.

Im Folgenden werden die notwendigen Prozessschritte genauer betrachtet.

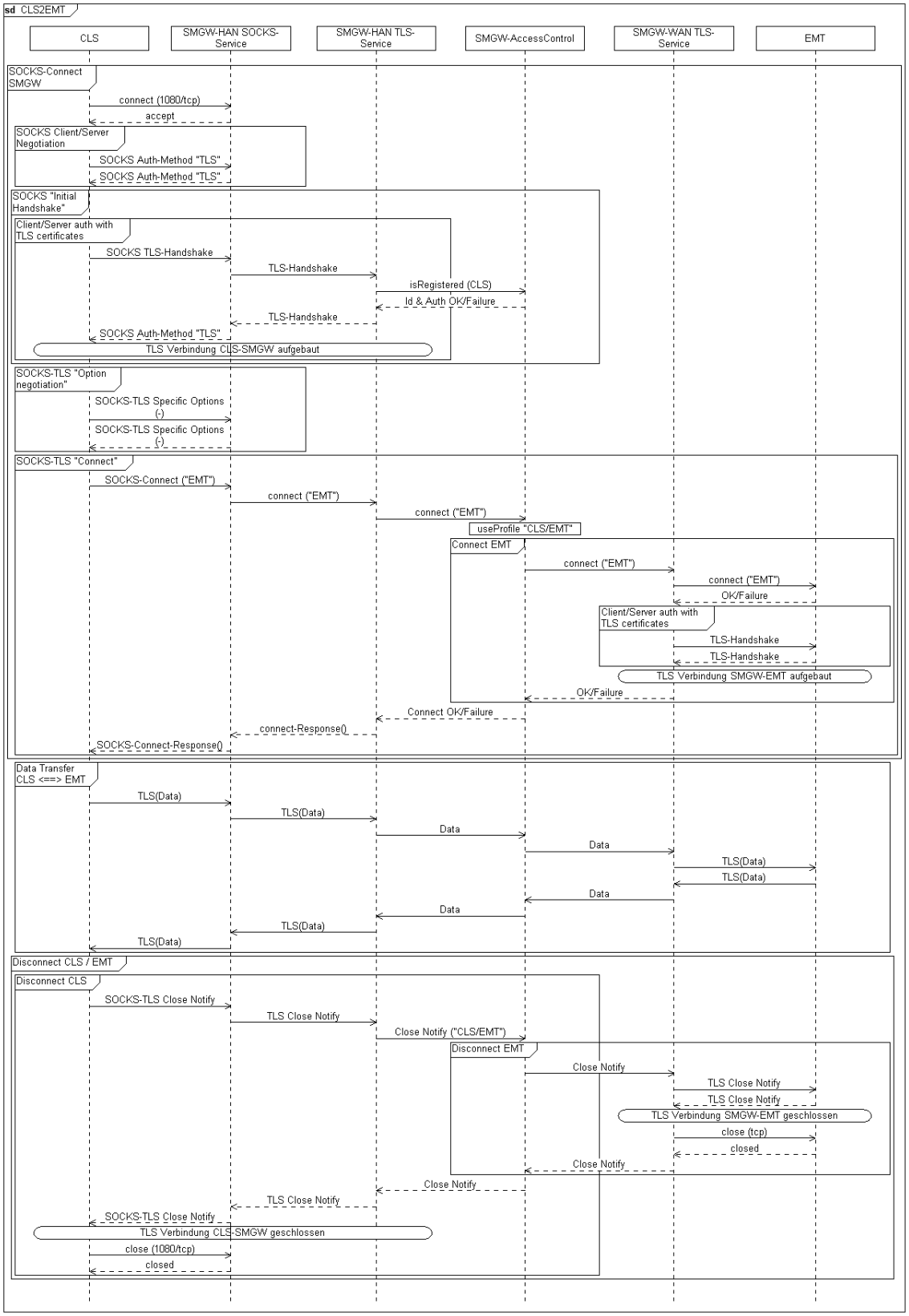

Abbildung 17: Sequenzdiagramm transparenter Kanal initiiert durch CLS

a) Aufbau einer SOCKSv5 Verbindung vom CLS zum SMGW (tcp/port 1080)

b) Vom CLS wird dabei die Authentication Method TLS[9] vorgeschlagen („Client Negotiation“).
c) Vom SOCKS-Server wird nur die „Method“ TLS akzeptiert (sonst Fehlermeldung) („Server Negotiation“).
d) Nächster Schritt ist die „Authentication“ mittels der methodenspezifischen Sub-Negotiation zwischen SOCKS Client und Server [DRAFT-IETF-AFT-SOCKS-SSL-00].
   i) Aufbau der HAN-TLS Verbindung von CLS zum SMGW (SOCKS-TLS „Initial handshake“ und „Option negotiation“).
   ii) TLS Client-Server Identifikation und Authentifizierung mit Hilfe der Zertifikate von CLS und SMGW.
   iii) Der etablierte TLS-Kanal wird für alle weiteren SOCKS-Nachrichten der Session verwendet (SOCKS- TLS „Data-Flow“).
e) Das CLS meldet per SOCKS-Connect die gewünschte Zieladresse EMT. („Client Request“)
f) Im Proxy-Kommunikationsprofil ist EMT als zulässiger Kommunikationspartner für das CLS festgelegt
   i) Aufbau der WAN-TLS Verbindung von SMGW zum EMT („Server Request/Response“)
   ii) TLS Client-Server Identifikation und Authentifizierung mit Hilfe der Zertifikate von SMGW und EMT
   iii) SOCKS-Connect-Response an CLS („Client Response“)
g) Transparente Datenkommunikation über die beiden etablierten TLS-Tunnel.
h) Beenden der Verbindung.

Notwendige Vorbedingungen

Akteur	Beschreibung
SMGW	SMGW-WAN: Das SMGW agiert als TLS Client und verfügt über ein eindeutiges WAN-Zertifikat GW_WAN_TLS_CRT. Das zugehörige Schlüsselmaterial ist im Sicherheitsmodul gespeichert. Dieses Zertifikat wird vom EMT genutzt, um das SMGW zu authentifizieren. SMGW-HAN: Das SMGW agiert als SOCKSv5-TLS Server und verfügt über ein eindeutiges HAN-Zertifikat GW_HAN_TLS_CRT. Das zugehörige Schlüsselmaterial ist im Sicherheitsmodul gespeichert. Dieses Zertifikat wird vom CLS genutzt, um das SMGW zu authentifizieren.

[9] Method-Id=0x06 gemäß IANA Assignments Socks-Methods (draft-ietf-aft-socks-ssl-00 verwendet Id=0x86).

Akteur	Beschreibung
	Proxy-Kommunikationsprofil: Die Zulässigkeit der Proxy-Verbindung und die Kommunikationsparameter für den Verbindungsaufbau zum EMT sind in einem Proxy-Kommunikationsprofil konfiguriert.
CLS	Das CLS agiert als ein SOCKSv5-TLS Client und **MUSS** über ein eindeutiges HAN-Zertifikat CLS_HAN_TLS_CRT verfügen. Dieses Zertifikat wird vom SMGW genutzt, um das CLS zu authentifizieren.
EMT	Der EMT agiert als TLS Server und **MUSS** über ein eindeutiges WAN-Zertifikat EMT_WAN_TLS_CRT verfügen. Dieses Zertifikat wird vom SMGW genutzt, um den EMT zu authentifizieren. Der EMT ist unter einem eindeutigen Bezeichner registriert, welcher zur Adressierung des EMT benutzt werden kann.

Tabelle 14: HKS3: Transparenter Kanal initiiert durch CLS

Ergebnis

Der gewünschte transparente Kanal wurde etabliert.

3.4.3.4 Kommunikationsszenario HKS4: Transparenter Kanal initiiert durch EMT

Beschreibung

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

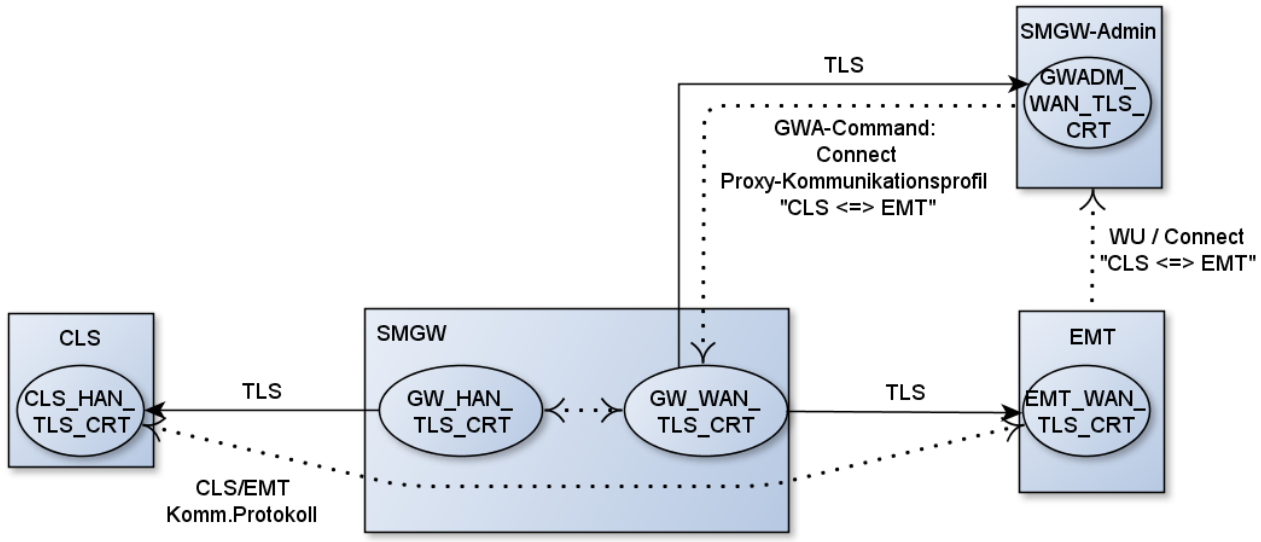

Abbildung 18: Transparenter Kanal initiiert durch EMT (über den SMGW-Admin)

Im Folgenden werden die notwendigen Prozessschritte genauer betrachtet.

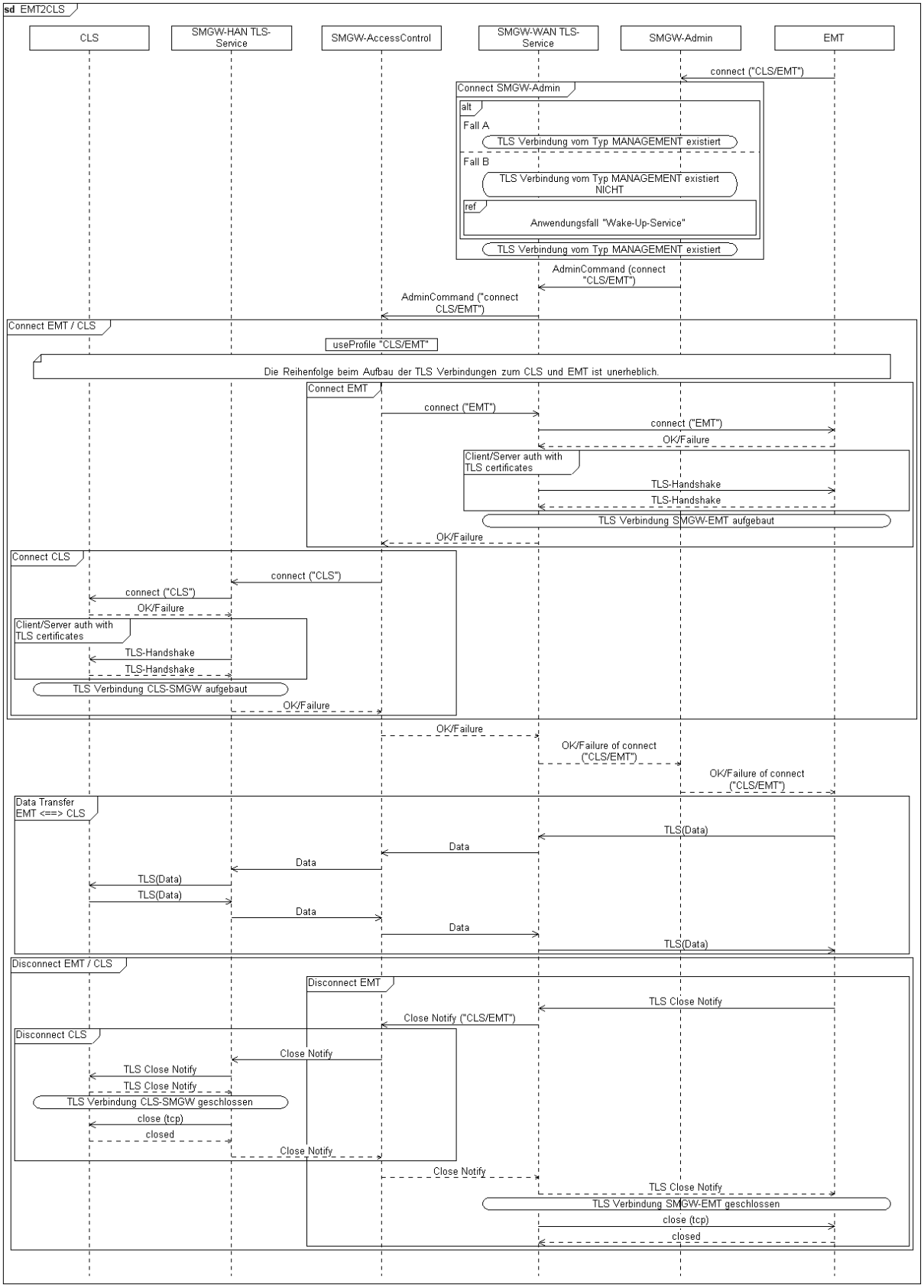

Abbildung 19: Sequenzdiagramm Transparenter Kanal initiiert durch EMT

a) Der EMT teilt die gewünschte Zieladresse des CLS dem SMGW Administrator (z.B. über einen Webservice) mit. Die Schnittstelle EMT⇔SMGW-Admin wird nicht durch diese TR festgelegt.
b) (Optional) Der SMGW-Admin schickt ein Wake-Up-Paket zum SMGW, damit dieses die TLS-Verbindung vom Typ „MANAGEMENT“ zum SMGW-Admin aufbaut.
c) Der SMGW-Admin sendet über die bestehende TLS-Verbindung den Administrationsbefehl „Connect Proxy-Kommunikationsprofil: CLS/EMT“ zum SMGW.
d) Auf dem SMGW ist im Proxy-Kommunikationsprofil der 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) HAN-Connect-Response an SMGW-Admin
f) Aufbau der WAN-TLS Verbindung vom SMGW zum EMT
   i) TLS Client-Server Identifikation und Authentifizierung mit Hilfe der Zertifikate von SMGW im WAN und des EMT Zertifikats.
   ii) WAN-Connect-Response an SMGW-Admin
g) (Optional) SMGW Administrator meldet den Connect-Response an den EMT (z.B. via eines Webservices). Alternativ kann der erfolgreiche TLS-Kanalaufbau im WAN als „OK“ gewertet werden.
h) Transparente Datenkommunikation über die beiden etablierten TLS-Tunnel
i) Beenden der Verbindung.

Notwendige Vorbedingungen

Akteur	Beschreibung
SMGW	SMGW-WAN: Das SMGW agiert als TLS Client und verfügt über ein eindeutiges WAN-Zertifikat GW_WAN_TLS_CRT. Das zugehörige Schlüsselmaterial ist im Sicherheitsmodul gespeichert. Dieses Zertifikat wird vom EMT genutzt, um das SMGW zu authentifizieren. SMGW-HAN: Das SMGW agiert als TLS Client und verfügt über ein eindeutiges HAN-Zertifikat GW_HAN_TLS_CRT. Das zugehörige Schlüsselmaterial ist im Sicherheitsmodul gespeichert. Dieses Zertifikat wird vom CLS genutzt, um das SMGW zu authentifizieren.

Akteur	Beschreibung
	Proxy-Kommunikationsprofil: Die Zulässigkeit der Proxy-Verbindung und die Kommunikationsparameter für den Verbindungsaufbau zum EMT und CLS sind in einem Proxy-Kommunikationsprofil konfiguriert.
SMGW-Admin	Der SMGW-Admin agiert als TLS Server und verfügt über ein eindeutiges WAN-Zertifikat GWADM_WAN_TLS_CRT Der SMGW-Admin kann ein Wake-Up-Paket für das SMGW erstellen und kennt die Kommunikationsparameter zur Zustellung dieses Pakets beim SMGW.
CLS	Das CLS agiert als TLS Server und **MUSS** über ein eindeutiges HAN-Zertifikat CLS_HAN_TLS_CRT verfügen. Dieses Zertifikat wird vom SMGW genutzt, um das CLS zu authentifizieren. Das CLS ist unter einem eindeutigen Bezeichner registriert, welcher zur Adressierung des CLS durch den EMT benutzt werden kann.
EMT	Der EMT agiert als TLS Server und **MUSS** über ein eindeutiges WAN-Zertifikat EMT_WAN_TLS_CRT verfügen. Dieses Zertifikat wird vom SMGW genutzt, um den EMT zu authentifizieren. Der EMT ist unter einem eindeutigen Bezeichner registriert, welcher zur Adressierung des EMT benutzt werden kann.

Tabelle 15: HKS4: Transparenter Kanal initiiert durch EMT

Ergebnis

Der gewünschte transparente Kanal wurde etabliert.

3.4.3.5 Kommunikationsszenario HKS5: Transparenter Kanal initiiert durch SMGW

Beschreibung

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

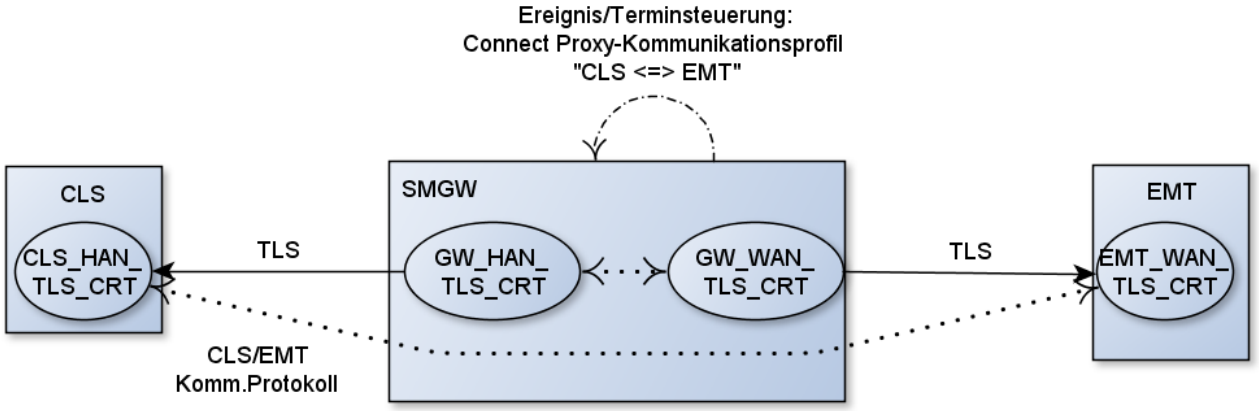

Abbildung 20: Transparenter Kanal initiiert durch das SMGW

Im Folgenden werden die notwendigen Prozessschritte genauer betrachtet.

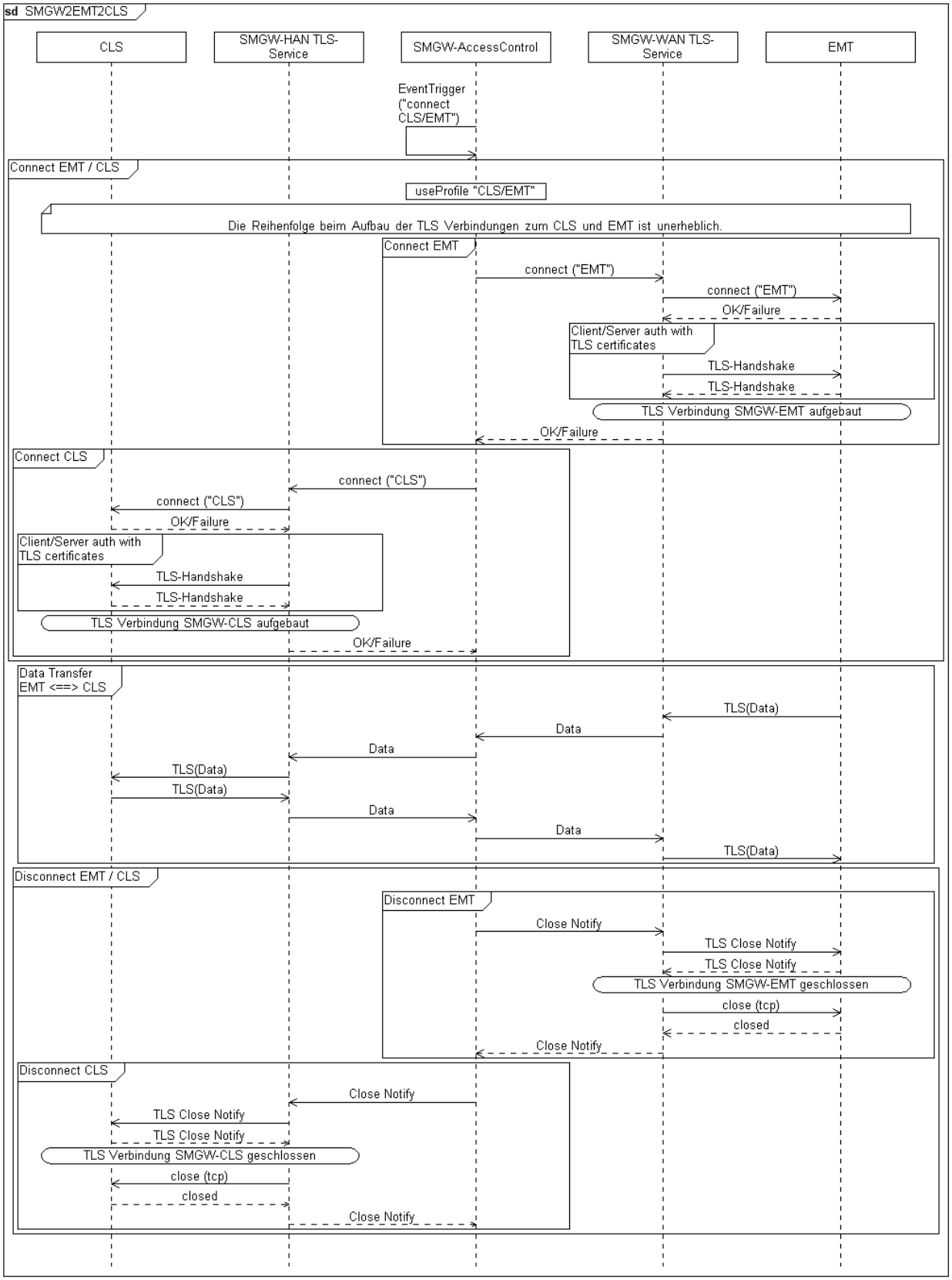

Abbildung 21: Sequenzdiagramm Transparenter Kanal initiiert durch SMGW

a) Auf dem SMGW ist im Proxy-Kommunikationsprofil der 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 EMT
   i) TLS Client-Server Identifikation und Authentifizierung mit Hilfe der Zertifikate von SMGW im WAN und des EMT Zertifikats.
   ii) WAN-Connect-Response an SMGW
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) HAN-Connect-Response an SMGW
d) Transparente Datenkommunikation über die beiden etablierten TLS-Tunnel
e) Beenden der Verbindung.

Notwendige Vorbedingungen

Akteur	Beschreibung
SMGW	SMGW-WAN: Das SMGW agiert als TLS Client und verfügt über ein eindeutiges WAN-Zertifikat GW_WAN_TLS_CRT. Das zugehörige Schlüsselmaterial ist im Sicherheitsmodul gespeichert. Dieses Zertifikat wird vom EMT genutzt, um das SMGW zu authentifizieren. SMGW-HAN: Das SMGW agiert als TLS Client und verfügt über ein eindeutiges HAN-Zertifikat GW_HAN_TLS_CRT. Das zugehörige Schlüsselmaterial ist im Sicherheitsmodul gespeichert. Dieses Zertifikat wird vom CLS genutzt, um das SMGW zu authentifizieren. Proxy-Kommunikationsprofil: Die Zulässigkeit der Proxy-Verbindung und die Kommunikationsparameter für den Verbindungsaufbau zum EMT und CLS sind in einem Proxy-Kommunikationsprofil konfiguriert.
CLS	Das CLS agiert als TLS Server und **MUSS** über ein eindeutiges HAN-Zertifikat CLS_HAN_TLS_CRT verfügen. Dieses Zertifikat wird vom SMGW genutzt, um das CLS zu authentifizieren.

Akteur	Beschreibung
	Das CLS ist unter einem eindeutigen Bezeichner registriert, welcher zur Adressierung des CLS benutzt werden kann.
EMT	Der EMT agiert als TLS Server und **MUSS** über ein eindeutiges WAN-Zertifikat EMT_WAN_TLS_CRT verfügen. Dieses Zertifikat wird vom SMGW genutzt, um den EMT zu authentifizieren. Der EMT ist unter einem eindeutigen Bezeichner registriert, welcher zur Adressierung des EMT benutzt werden kann.

Tabelle 16: HKS5: Transparenter Kanal initiiert durch das SMGW

Ergebnis

Der gewünschte transparente Kanal wurde etabliert.

3.4.4 Sicherung der Kommunikationsverbindungen in das HAN

Gemäß den Anforderungen aus dem Schutzprofil [GW_PP] **MÜSSEN** die Kommunikationsverbindungen des SMGW in das HAN oberhalb der Transportschicht mittels TLS abgesichert werden.

3.4.4.1 Sicherung der Kommunikation mit dem Letztverbraucher / Service-Techniker

Das SMGW **MUSS** einen TLS gesicherten Kanal für die sichere Kommunikation mit der Anzeigeeinheit/CLS des Letztverbrauchers/ Service-Technikers anbieten.

Erst nach erfolgreicher Authentifizierung des Letztverbrauchers oder Service-Technikers erfolgt eine Übermittlung von Daten durch das SMGW. Es **DÜRFEN** nur die Daten übermittelt werden, die im SMGW dem authentifizierten Letztverbraucher bzw. Service-Techniker zugeordnet sind.

Das SMGW **MUSS** einem Letztverbraucher bzw. Service-Techniker eine Funktion zum sicheren Ausloggen bereitstellen. Weiterhin **MUSS** das SMGW den Letztverbraucher automatisch ausloggen, sobald dieser über einen konfigurierten Zeitraum hinaus inaktiv war.

3.4.4.2 Sicherung der Kommunikation zwischen CLS und EMT

Das SMGW **MUSS** eine sichere Kommunikation zwischen CLS im HAN und konfigurierten EMT im WAN ermöglichen. Hierzu **MUSS** das SMGW eine Proxy Funktionalität bereitstellten, die eine

gesicherte Verbindung des SMGW mit einem CLS auf eine gesicherte Verbindung des SMGW mit einem EMT abbildet. Dies illustriert die folgende Abbildung.

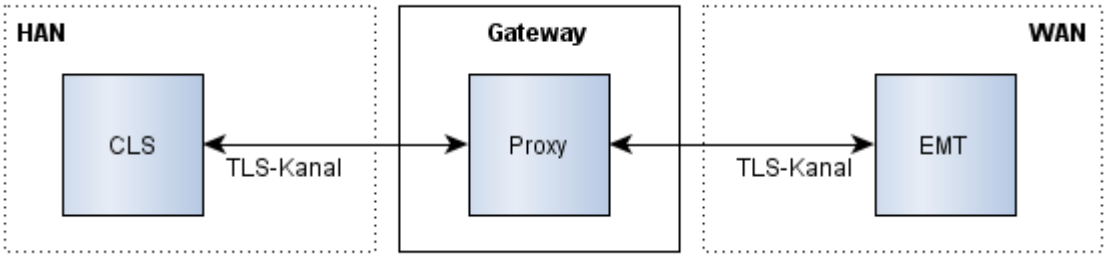

Abbildung 22: Absicherung der Kommunikation zwischen CLS und EMT

Für die Kommunikation mit dem EMT im WAN **MUSS** das SMGW immer in der Rolle des TLS-Client und die Gegenstelle in der Rolle des TLS-Servers agieren. Dabei **MUSS** immer beidseitig mit Zertifikaten authentifiziert werden. Die WAN Zertifikate **MÜSSEN** aus der Smart Metering Public Key Infrastruktur [BSI TR-03109-4] stammen.

Für die Kommunikation zwischen CLS und dem SMGW **MUSS** immer ein beidseitig auf Zertifikaten basierender authentifizierter TLS-Kanal aufgebaut werden. Das CLS und das SMGW **MÜSSEN** sowohl als TLS-Client als auch als TLS-Server agieren können.

3.4.4.3 Identifizierung und Authentifizierung

Das SMGW **MUSS** sicherstellen, dass zur Identifizierung und Authentifizierung von Service-Technikern und CLS gegenüber dem SMGW ausschließlich HAN-Zertifikate verwendet werden.

Des Weiteren muss das SMGW die Identifizierung und Authentifizierung von Letztverbrauchern gegenüber dem SMGW mittels HAN-Zertifikaten und mittels Kennung und Passwort ermöglichen.

Das SMGW **MUSS** sich immer mit seinem HAN Zertifikat GW_HAN_TLS_CRT authentifizieren. Das SMGW **MUSS** die clientseitige Identifizierung und Authentifizierung entweder mittels Zertifikat und/oder mittels Kennung und Passwort gemäß HTTP Digest Access Authentication [RFC2617] durchsetzen.

Die Benutzeridentitäten (Letztverbraucher, Service-Techniker, CLS und deren Zertifikate bzw. Kennung und Passwörter) **MÜSSEN** auf dem SMGW registriert bzw. konfiguriert werden, damit diese vom SMGW als vertrauenswürdig akzeptiert werden. Einem Letztverbraucher **KÖNNEN** durchaus mehrere Zertifikate bzw. Kennungen und Passworte zugeordnet sein (z.B. mehrere Anzeigeeinheiten, CLS mit Datenzugriff, usw.).

Die HAN-Zertifikate sind selbst-signiert oder sind von einer herstellerspezifischen CA bzw. einer eigenen SMGW-Admin CA ausgestellt worden.

Die Zertifikate **MÜSSEN** die Kryptoanforderungen aus [BSI TR-03109-3] erfüllen. Details zu den Zertifikaten sind in „Anhang C: Zertifikate im HAN“ definiert.

3.4.5 Technische Anforderungen an die HAN-Schnittstelle

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

Das SMGW **MUSS** IPv4 und es **KANN** IPv6 unterstützen. Die Adresskonfiguration **SOLLTE** über DHCP bzw. DHCPv6 (SMGW als Client) oder manuell erfolgen. „Dynamic Configuration of IPv4 Link-Local Addresses“ bzw. „IPv6 Stateless Address Autoconfiguration“ **KANN** unterstützt werden.

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

Weitere HAN-Schnittstellen, die den obigen Anforderungen genügen, **KÖNNEN** am SMGW bereitgestellt werden.

3.4.6 Kommunikationsprofile im HAN

3.4.6.1 Einleitung

Dieses Kapitel hat informativen Charakter.

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

3.4.6.2 HAN-Kommunikationsprofile

HAN-Kommunikationsprofile legen die Parameter für die Kommunikation des SMGW zu Letztverbrauchern oder Service-Technikern fest.

HAN-Kommunikationsprofile **MÜSSEN** zumindest die folgenden Parameter beinhalten:

Parameter	***Datentyp / Wertebereich[10]***	***Beschreibung***
Bezeichner	Text	Der im SMGW eindeutige Bezeichner des HAN-Kommunikationsprofils.
Name	Text	Ein detaillierter Name für das HAN-Kommunikationsprofil.

[10] Die hier dargestellten Datentypen und Wertebereiche besitzen informativen Charakter.

Parameter	***Datentyp / Wertebereich[10]***	***Beschreibung***
Letztverbraucher- bzw. Service-Techniker-Kennung	Text	Eindeutiger Bezeichner für den Letztverbraucher bzw. für den Service-Techniker.
Rolle	Einer aus: Letztverbraucher Service-Techniker	Legt die Rolle des Letztverbrauchers fest.
Schnittstelle	Einer aus: IF_GW_CON IF_GW_SRV	Legt die logische Schnittstelle des SMGW fest, über die der Letztverbraucher, der Service-Techniker oder CLS, die eine Freigabe durch den Letztverbraucher erhalten haben, erreichbar sind.
Kommunikationsszenario gemäß Kapitel 3.4.3	Einer aus: HKS1 HKS2	Legt das Kommunikationsszenario gemäß Kapitel 3.4.3 fest.
Adresse(n) des Kommunikationspartners im HAN	1..n URI	Legt eine oder mehrere Adressen fest, über die der Kommunikationspartner erreichbar ist und zu der ein TLS-Kanal vom SMGW aufgebaut werden kann.
Keepalive	Bool / Ja/Nein	Legt fest, ob der TLS-Kanal 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	0..n	Anzahl der TLS-Kanalaufbauversuche im Fehlerfall. Führen alle Versuche zu einem Fehler, so muss das Ereignis im System-Log eingetragen werden.
Wartezeit im Fehlerfall	0..n Sekunden	Die Wartezeit zwischen Kanalaufbauversuchen.
Wartezeit im Leerlauf	0..n Sekunden	Nach Ablauf der Zeit im Leerlauf, wird der TLS-Kanal wieder abgebaut. Der Wert 0 deaktiviert den Abbau im Leerlauf.

Parameter	***Datentyp / Wertebereich[10]***	***Beschreibung***
Maximale Sitzungslänge	0..172800 Sekunden	Die maximale Zeit, die ein TLS-Kanal aufgebaut bleiben soll. Ein Wert größer als 48h darf vom SMGW nicht akzeptiert werden.
Zertifikat des Kommunikationspartners für die TLS-Authentifizierung (in Abhängigkeit des Kommunikationsszenarios)	CON_HAN_TLS_CRT	Das Zertifikat des Kommunikationspartners für die TLS-Authentifizierung des Kommunikationspartners durch das SMGW. Ist im Kommunikationsszenario kein Zertifikat vorgesehen, so hat in diesem Feld der Eintrag „none“ zu erfolgen.
Kennung + Passwort (in Abhängigkeit des Kommunikationsszenarios)	Text	Kennung und Passwort gemäß HTTP Digest Access Authentication falls im Kommunikationsszenario gefordert. Das Passwort **MUSS** den Anforderungen aus [BSI-TR-03109-3] genügen. Ist im Kommunikationsszenario ein Zertifikat vorgesehen, so hat in diesem Feld der Eintrag „none“ zu erfolgen.
Zertifikat des SMGW für die TLS-Authentifizierung	GW_HAN_TLS_CRT	Ein Zertifikat des SMGW für die TLS-Authentifizierung durch den Kommunikationspartner.
Privater Schlüssel des SMGW für die TLS-Authentifizierung	Key-ID des Sicherheitsmoduls	Eine Referenz auf einen Schlüssel im Sicherheitsmodul, der für die TLS-Authentifizierung des SMGW verwendet werden muss.

Tabelle 17: Durch HAN-Kommunikationsprofile festzulegende Parameter

Das SMGW **KANN** weitere Parameter für HAN-Kommunikationsprofile unterstützen.

HAN-Kommunikationsprofile **MÜSSEN** ausschließlich vom SMGW Administrator eingespielt werden können. Vor der Aktivierung des HAN-Kommunikationsprofils **MUSS** das SMGW die folgenden Punkte sicherstellen:

- Die referenzierten Key-IDs existieren im Sicherheitsmodul.
- Ist als Rolle der Service-Techniker festgelegt, so **MUSS** als Schnittstelle IF_GW_SRV und als Kommunikationsszenario HKS2 eingetragen sein.
- Ist als Rolle der Letztverbraucher festgelegt, so **MUSS** als Schnittstelle IF_GW_CON eingetragen sein.

3.4.6.3 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 (siehe Kapitel 3.4.3) 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.

Proxy-Kommunikationsprofile **MÜSSEN** zumindest die folgenden Parameter beinhalten:

Parameter	***Datentyp / Wertebereich[11]***	***Beschreibung***
Bezeichner	Text	Der im SMGW eindeutige Bezeichner des Proxy-Kommunikationsprofil.
Name	Text	Ein Name für das Proxyprofil.
CLS-ID	Text	Eindeutiger Bezeichner des CLS.
EMT-Kennung	Text	Eindeutiger Bezeichner des EMT.
GültigVon	Datum+Uhrzeit [UTC]	Das Proxyprofil ist aktiv ab dem konfigurierten Zeitpunkt. Ein leeres Feld bedeutet: Keine Begrenzung vorgesehen.
GültigBis	Datum+Uhrzeit [UTC]	Das Proxyprofil ist aktiv bis zum konfigurierten Zeitpunkt. Ein leeres Feld bedeutet: Keine Begrenzung vorgesehen.
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.
Kommunikationsszenario gemäß Kapitel 3.4.3	HKS3 HKS4 HKS5	Legt das Kommunikationsszenario gemäß Kapitel 3.4.3 fest.

[11] Die hier dargestellten Datentypen und Wertebereiche besitzen informativen Charakter.

Parameter	***Datentyp / Wertebereich[11]***	***Beschreibung***
CLS-Proxy Priorität	Text	Das Feld CLS-Proxy Priorität bietet die Möglichkeit zu definieren, welches Proxyprofil und damit welcher EMT Vorrang bekommt bei Konfliktsituationen zwischen mehreren Proxy Verbindungen.
Proxy-Start-Ereignis		Legt das Ereignis fest, bei dem eine Proxy-Verbindung 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	Bool / Ja/Nein	Legt fest, ob der TLS-Kanal 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	0..n	Anzahl der TLS-Kanalaufbauversuche im Fehlerfall. Führen alle Versuche zu einem Fehler, so muss das Ereignis im System-Log eingetragen werden.
Wartezeit im Fehlerfall	0..n Sekunden	Die Wartezeit zwischen Kanalaufbauversuchen.
Wartezeit im Leerlauf	0..n Sekunden	Nach Ablauf der Zeit im Leerlauf, wird der TLS-Kanal wieder abgebaut. Der Wert 0 deaktiviert den Abbau im Leerlauf.
Maximale Sitzungslänge	0..172800 Sekunden	Die maximale Zeit, die ein TLS-Kanal aufgebaut bleiben soll. Ein Wert größer als 48h darf vom SMGW nicht akzeptiert werden.
Zertifikat des Kommunikationspartners EMT für die TLS-Authentifizierung	EMT_WAN_TLS_CRT	Das Zertifikat des Kommunikationspartners für die TLS-Authentifizierung des Kommunikationspartners EMT durch das SMGW.

Parameter	***Datentyp / Wertebereich[11]***	***Beschreibung***
Zertifikat des Kommunikationspartners CLS für die TLS-Authentifizierung	CLS_HAN_TLS_CRT	Das Zertifikat des Kommunikationspartners 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.
Privater Schlüssel des SMGW für die TLS-Authentifizierung im WAN	Key-ID des Sicherheitsmoduls	Eine Referenz auf einen Schlüssel im Sicherheitsmodul, der für die TLS-Authentifizierung des SMGW im WAN verwendet werden muss.
Privater Schlüssel des SMGW für die TLS-Authentifizierung im HAN	Key-ID des Sicherheitsmoduls	Eine Referenz auf einen Schlüssel im Sicherheitsmodul, der für die TLS-Authentifizierung des SMGW im HAN verwendet werden muss.

Tabelle 18: Durch Proxy-Kommunikationsprofile festzulegende Parameter

Proxy-Kommunikationsprofile werden über den Profilbezeichner referenziert. Zu einem Zeitpunkt **DÜRFEN NICHT** mehrere Proxy-Kommunikationsprofile für ein bestimmtes Tupel der Kommunikationspartner EMT und CLS aktiv sein.

Das SMGW **KANN** weitere Parameter für Proxy-Kommunikationsprofile unterstützen.

Proxy-Kommunikationsprofile **MÜSSEN** nur vom SMGW Administrator eingespielt werden können.

4 Messwertverarbeitung für Tarifierung, Bilanzierung und Netzzustandsdatenerhebung

4.1 Einleitung

Dieses Kapitel hat informativen Charakter.

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. Des Weiteren legt dieses Kapitel dar, wie Messwerte für eine zentrale Tarifierung zur Verfügung gestellt werden können. Regelwerke im SMGW bestimmen, wie Messwerte für Auswertungen verwendet werden.

In diesem Kapitel werden Mindestanforderungen an die Messwertverarbeitung gestellt.

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

4.2 Anwendungsfälle für Regelwerke

4.2.1 Einleitung

Dieses Kapitel beschreibt die Anwendungsfälle für Tarifierung, Bilanzierung und Netzzustandsdatenerhebung, die als Minimalanforderung vom SMGW durch Regelwerke umgesetzt werden **MÜSSEN**. 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
- Der beim Anwendungsfall zu ermittelnde und an externe Marktteilnehmer zu versendende Messwertsatz
- Die vom SMGW für den Letztverbraucher an der HAN-Schnittstelle als Minimum bereitzustellenden Daten

4.2.2 Anwendungsfälle für die Tarifierung und Bilanzierung

4.2.2.1 TAF1: Datensparsame Tarife (nach § 40 (5) EnWG)

4.2.2.1.1 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 Letztverbrauchers getätigt werden können. Der Anwendungsfall betrachtet nur eine Tarifstufe. Es ist dabei möglich, die Zählerstände mehrerer Zähler eines Letztverbrauchers zu addieren bzw. zu subtrahieren und als Gesamtverbrauch bzw. -einspeisung zu versenden.

Zu diesem Zwecke versendet das SMGW von einem oder mehreren relevanten angeschlossenen Zählern jeweils nur einen Zählerstand pro Abrechnungszeitraum an autorisierte externe Marktteilnehmer. Der Abrechnungszeitraum ist dabei nicht kürzer als ein Monat zu wählen. Die Zählerstände werden in der zugeordneten Messwertliste eingetragen.

Zeitstempel	***Grund***[12]	***Zählerstand Zähler 1 in kWh***	***Zählerstand Zähler 2 in kWh***	***…***
01.02.2013 0:00:00h	Monatliche Ablesung	512	124	…
01.03.2013 0:00:00h	Monatliche Ablesung	545	134	…
01.04.2013 0:00:00h	Monatliche Ablesung	567	154	…
01.05.2013 0:00:00h	Monatliche Ablesung	577	161	…
…	…	…	…	…

Tabelle 19: Beispiel für eine Messwertliste für einen einfachen Tarif mit minimalem Datenversand und zwei Zählern bei monatlicher Abrechnung

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

Zu den definierten Versandzeitpunkten werden die Summe der erfassten Zählerstände an die berechtigte Marktteilnehmer versendet. Über Zugriffsberechtigungen wird geregelt, welcher Marktteilnehmer berechtigt ist.

Das SMGW muss die in diesem Anwendungsfall zu versendenden Daten vor der Inhaltsdatenverschlüsselung mit einer zusätzlichen Signatur versehen (siehe Kapitel 3.2.4.4).

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

Der Letztverbraucher ist berechtigt die aktuellen und bereits versendeten Messwerte über die HAN-Schnittstelle einzusehen (vgl. Kapitel 3.4.2.1). Über eine Letztverbraucherkennung ist der Tarif mit dem Letztverbraucher verknüpft.

Ein Gültigkeitszeitraum legt fest, ab welchen Zeitpunkt das Regelwerk in Betrieb gehen soll und zu welchem Zeitpunkt es den Betrieb wieder einstellen soll.

4.2.2.1.2 Notwendige Parameter für das Regelwerk

Parameter	***Beschreibung***
Geräte-IDs der Zähler	Die eindeutigen Bezeichner der Zähler.
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 des Zählpunktes.
Abrechnungszeitraum	Der Zeitraum für den ein Messwertsatz für die Abrechnung ermittelt werden muss.
Letztverbraucherkennung	Die eindeutige Kennung des Letztverbrauchers, der die angefallenen Daten einsehen darf.
Zugriffsberechtigungen	Zugriffsberechtigungen, 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 20: Regelwerkparameter für TAF1

4.2.2.1.3 Vom Regelwerk für externe Marktteilnehmer bereitzustellender Messwertsatz

Der zu ermittelnde Messwertsatz enthält die Summe der Zählerstände am Ende des jeweiligen Abrechnungszeitraums.

4.2.2.1.4 Für den jeweiligen Letztverbraucher an der HAN-Schnittstelle bereitzustellende Daten

- Alle Parameter des Regelwerks
- Die aktuellen Zählerstände und deren Summe, sowie Differenzbeträge zum Ende des letzten Abrechnungszeitraums (mindestens 15-minutengenau für Strom und 60-minutengenau für Gas)
- Die bereits versendeten Zählerstände und deren Summe zum Ende eines jeden Abrechnungszeitraumes innerhalb des letzten Jahres
- Die bereits versendeten Zählerstände und deren Summe des jeweils letzten Abrechnungszeitraums in den vergangenen 3 Jahren (Jahreswerte)
- Die Messwertliste

4.2.2.2 TAF2: Zeitvariable Tarife (nach § 40 (5) EnWG)

4.2.2.2.1 Beschreibung

Das SMGW ermöglicht den Anwendungsfall, bei dem der Lieferant dem Letztverbraucher für unterschiedliche Zeiträume verschiedene Preise für die in den jeweiligen Zeiträumen angefallenen Energiemengen in Rechnungen stellt. Die jeweiligen Energiemengen können dann beim Lieferanten separiert mir Preisen versehen und abgerechnet werden

Hierzu werden im SMGW mehrere Tarifstufen definiert, an denen jeweils eine Zeitbedingung geknüpft ist. Die Zeitbedingungen der Tarifstufen werden über Tarifumschaltzeitpunkte definiert. Zu jedem Zeitpunkt ist jeweils nur eine Tarifstufe pro Anwendungsfall aktiv. Für jede Tarifstufe wird vom SMGW die Energiemenge kumuliert, die anfällt, während die Tarifstufe aktiv ist. Die gesamte Energiemenge innerhalb des Abrechnungszeitraumes wird so auf mehrere Tarifstufen verteilt.

Bei Eintritt eines Tarifumschaltzeitpunktes erfasst das SMGW die Zählerstände von einem oder mehreren Zählern, erzeugt einen Eintrag in der Messwertliste (s. Kapitel 4.3.3) und kumuliert die am Zähler (oder den Zählern) zwischen den letzten beiden Umschaltzeitpunkten angefallene Energiemenge zu der zuletzt gültigen Tarifstufe. (Beispiel für Entwicklung von Tarifstufen bei HT/NT-Tarifen s. Abbildung 23).

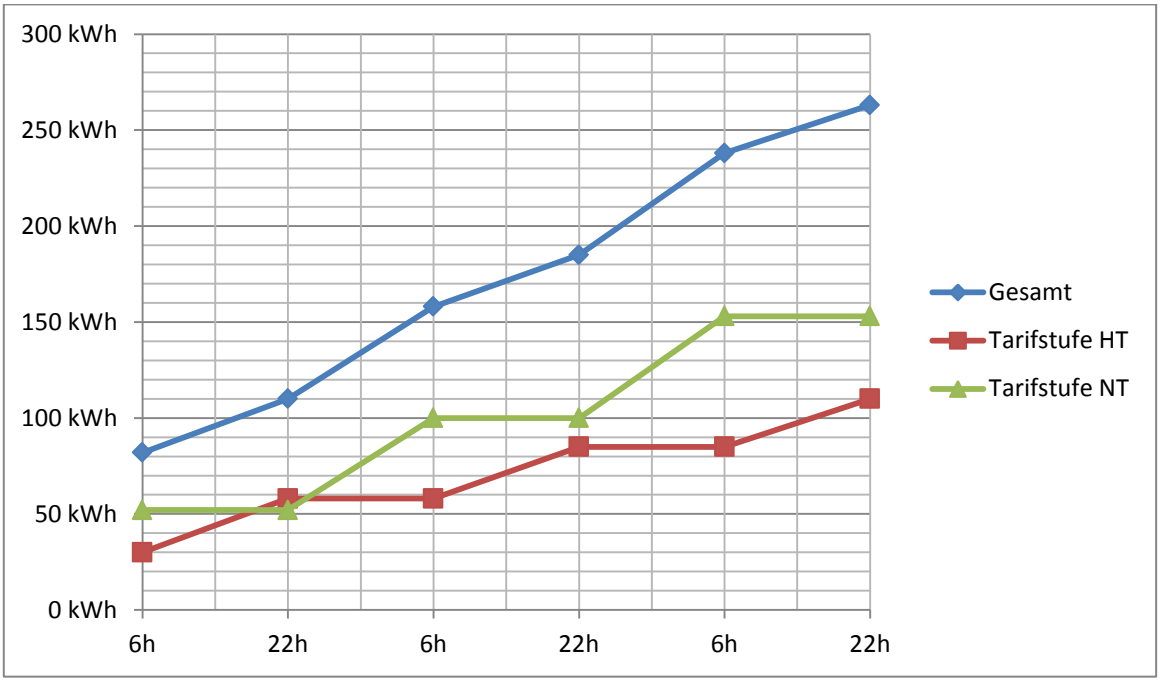

Abbildung 23: Beispiel für zeitvariable Tarife mit zwei Tarifstufen (HT/NT) und einem Zähler

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

Zu definierten Versandzeitpunkten werden die Zählerstände der Tarifstufen dann an berechtigte Marktteilnehmer versendet. Für die Bilanzierung kann zusätzlich die Tarifwechselliste versendet werden, um die tarifierten Energiemengen tarifrichtig auf die zugehörigen Zeitabschnitte verteilen

zu können. Über Zugriffsberechtigungen wird geregelt, welcher Marktteilnehmer berechtigt ist. Nach dem Versenden der Zählerstände können bei dem berechtigten Marktteilnehmer für unterschiedliche Tarifstufen verschiedene Preise in Rechnungen gestellt werden.

Das SMGW muss die in diesem Anwendungsfall zu versendenden Daten vor der Inhaltsdatenverschlüsselung mit einer zusätzlichen Signatur versehen (siehe Kapitel 3.2.4.4).

Der Letztverbraucher ist berechtigt die aktuellen und bereits versendeten Messwerte über die HAN-Schnittstelle einzusehen (vgl. Kapitel 3.4.2.1). Über eine Letztverbraucherkennung ist der Tarif mit dem Letztverbraucher verknüpft. Der Letztverbraucher kann alle Parameter des Regelwerks einsehen. Auf diese Weise erhält er auch lesenden Zugriff auf die künftigen Tarifumschaltzeitpunkte, die er so in sein Energiemanagement einbeziehen kann.

Ein Gültigkeitszeitraum legt fest, ab welchen Zeitpunkt das Regelwerk in Betrieb gehen soll und zu welchem Zeitpunkt es den Betrieb wieder einstellen soll.

Hinweis: 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 eingespeiste Energiemengen anstatt für verbrauchte Energiemengen. Weiterhin können Zähler für verbrauchte und eingespeiste Energiemengen auch zusammen veranlagt werden.

4.2.2.2.2 Notwendige Parameter für das Regelwerk

Parameter	***Beschreibung***
Geräte-IDs der Zähler	Die eindeutigen Bezeichner der Zähler.
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 des Zählpunktes.
Definition der Tarifstufen	Definiert die verschiedenen Tarifstufen und die zugehörigen OBIS-Kennzahlen. Hier wird auch definiert, welche Tarifstufe zum Zeitpunkt der Aktivierung des Regelwerks gültig ist.
Tarifumschaltzeitpunkte	Tarifumschaltzeitpunkte definieren die sekundengenauen Zeitpunkte, zu denen in eine andere Tarifstufe gewechselt werden muss. Die Zeitpunkte können periodisch wiederkehrend definiert sein.
Abrechnungszeitraum	Der Zeitraum für den ein Messwertsatz für die Abrechnung ermittelt werden muss.
Letztverbraucherkennung	Die eindeutige Kennung des Letztverbrauchers, der die angefallenen Daten einsehen darf.
Zugriffsberechtigungen	Zugriffsberechtigungen, 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.

Parameter	*Beschreibung*
Gültigkeitszeitraum	Der Zeitraum für den das Regelwerk im SMGW verwendet werden soll.

Tabelle 21: Regelwerkparameter für TAF2

4.2.2.2.3 Vom Regelwerk für externe Marktteilnehmer bereitzustellender Messwertsatz

- Für jede Tarifstufe: kumulierte Energiemenge zum Ende des Abrechnungszeitraums, die sich gemäß den Tarifumschaltzeitpunkten für die Tarifstufe ergeben.
- Bei Bedarf: Tarifwechselliste (für Bilanzierung)

4.2.2.2.4 Für den jeweiligen Letztverbraucher an der HAN-Schnittstelle bereitzustellende Daten

- Alle Parameter des Regelwerks
- Die aktuellen Zählerstände und die kumulierte Energie je Tarifstufe, sowie Differenzbeträge zum Ende des letzten Abrechnungszeitraums (mindestens 15-minutengenau für Strom und 60-minutengenau für Gas)
- Die Zählerstände und Stände der Tarifstufen zum Ende eines jeden Abrechnungszeitraumes innerhalb des letzten Jahres
- Die Messwertliste (Tarifwechselliste mit Zählerständen und den zugehörigen abgeleiteten Registern)
- Alle an externe Marktteilnehmer versendete Daten

4.2.2.3 TAF3: Lastvariable Tarife

4.2.2.3.1 Beschreibung

Das SMGW ermöglicht den Anwendungsfall, bei dem der Lieferant dem Letztverbraucher flexibel auf Basis der konkret anfallenden Last den Verbrauch zu unterschiedlichen Preisen in Rechnung stellt.

Hierzu werden mehrere Laststufen definiert, an denen jeweils eine Lastschwelle geknüpft ist. Eine Laststufe ist aktiv, wenn die Last die entsprechende Lastschwelle über- bzw. unterschreitet und keine weitere Laststufe existiert, die eine höhere bzw. niedrigere Lastschwelle besitzt, die auch über- bzw. unterschritten wird. Die Last kann dabei mithilfe des Leistungsmittelwertes oder auf Basis der Momentanleistung, soweit dies mit den eichtechnischen Richtlinien vereinbar ist, über eine definierte Registrierperiode bestimmt werden.

Bei Betrachtung der Momentanleistung wird genau dann in eine höhere Laststufe geschaltet, wenn die aktuelle vom Zähler gemessene Leistung die zugehörige Lastschwelle überschreitet. In eine niedrigere Laststufe wird geschaltet, wenn die aktuelle Leistung des Zählers die zugehörige Lastschwelle unterschreitet. Die Energiemenge und die Momentanleistung müssen im Takt der Registrierperiode erfasst werden. Die Registrierperiode muss dabei den eichtechnischen Anforderungen entsprechen. Das SMGW muss Registrierperioden von mindestens 15 Minuten unterstützen.

Wird für die Bestimmung der Last der Leistungsmittelwert herangezogen, so wird dieser mithilfe der Zählerstände zum Beginn und zum Ende der durch die Parametrierung definierten Registrierperiode bestimmt. Der Leistungsmittelwert bezieht sich dann auf den Zeitpunkt zum Ende der jeweiligen Registrierperiode. In diesem Fall wird genau dann in eine höhere Laststufe geschaltet, wenn der Leistungsmittelwert, der am Ende der Registrierperiode ermittelt wird, die zugehörige Lastschwelle überschreitet. In eine niedrigere Laststufe wird geschaltet, wenn der Leistungsmittelwert die zugehörige Lastschwelle unterschreitet.

Zu jedem Zeitpunkt ist jeweils nur eine Laststufe pro Anwendungsfall aktiv. Für jede Laststufe wird vom SMGW die Energiemenge kumuliert, die anfällt, während die entsprechende Laststufe aktiv ist. Die gesamte Energiemenge wird so auf mehrere Laststufen verteilt.

Erfolgt eine Umschaltung in eine der anderen Laststufen, erzeugt das SMGW einen entsprechenden Eintrag in der Messwertliste (s. Kapitel 4.3.3).

Zeitstempel	***Grund***[13]	***Zählerstand in kWh***	***Leistungsmittelwert in kW***	***…***
01.01.2013 9:00:00h	Umschaltung in Laststufe 2	10	6	…
01.01.2013 09:15:00h	Umschaltung in Laststufe 1	12	4	…
01.01.2013 09:45:00h	Umschaltung in Laststufe 2	14	7	…
01.01.2013 10:45:00h	Umschaltung in Laststufe 1	21	2	…
01.01.2013 11:15:00h	Umschaltung in Laststufe 2	22	8	…
01.01.2013 11:30:00h	Umschaltung in Laststufe 1	24	4	…
…	…	…	…	…

Tabelle 22: Beispiel für eine Messwertliste für lastvariablen Stromtarif mit zwei Laststufen und einem Zähler

Abbildung 24 zeigt den zugehörigen Verlauf des Gesamtverbrauches und der anteiligen Verbräuche in zwei Laststufen.

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

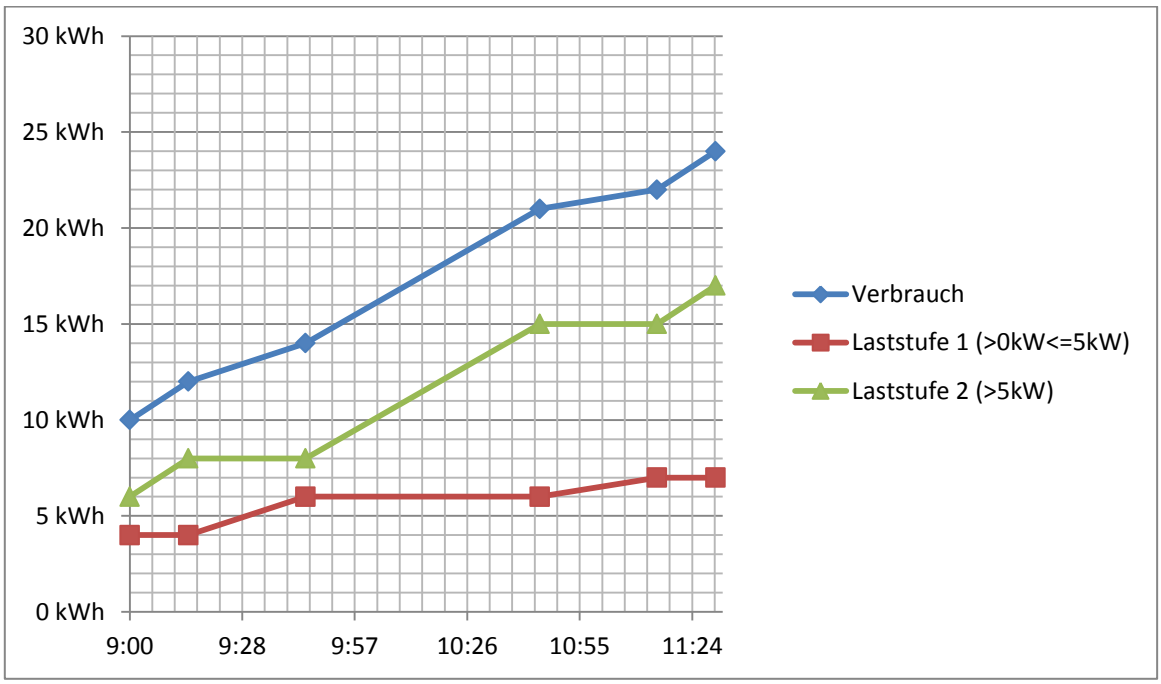

Abbildung 24: Beispiel für einen lastvariablen Tarif mit zwei Laststufen und einem Zähler

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

Zu definierten Versandzeitpunkten werden die Zählerstände der Laststufen dann an berechtigte Marktteilnehmer versendet. Über Zugriffsberechtigungen wird geregelt, welcher Marktteilnehmer berechtigt ist.

Das SMGW muss die in diesem Anwendungsfall zu versendenden Daten vor der Inhaltsdatenverschlüsselung mit einer zusätzlichen Signatur versehen (siehe Kapitel 3.2.4.4).

Der Letztverbraucher ist berechtigt die aktuellen und bereits versendeten Messwerte über die HAN-Schnittstelle einzusehen (vgl. Kapitel 3.4.2.1). Über eine Letztverbraucherkennung ist der Tarif mit dem Letztverbraucher verknüpft.

Ein Gültigkeitszeitraum legt fest, ab welchen Zeitpunkt das Regelwerk in Betrieb gehen soll und zu welchem Zeitpunkt es den Betrieb wieder einstellen soll.

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

4.2.2.3.2 Notwendige Parameter für das Regelwerk

Parameter	***Beschreibung***
Geräte-ID des Zählers	Der eindeutige Bezeichner des Zählers.
OBIS-Kennzahl der zu verwendenden Messgröße für die	Die eindeutige Kennzahl der für den Tarif zu verwendenden Messgröße des Zählers, die die verbrauchte oder eingespeiste

Parameter	***Beschreibung***
Energiemenge	Energiemenge angibt.
OBIS-Kennzahl der zu verwendenden Messgröße für die aktuelle Leistung	Die eindeutige Kennzahl der für den Tarif zu verwendenden Messgröße des Zählers, die die aktuelle Leistung angibt.
Zählpunktbezeichnung	Der eindeutige Bezeichner des Zählpunktes.
Definition der Laststufen	Definiert die verschiedenen Laststufen und deren Lastschwellen, sowie die zugehörigen OBIS-Kennzahlen. Hier wird auch definiert, welche Laststufe zum Zeitpunkt der Aktivierung des Regelwerks gültig ist.
Registrierperiode	Die Registrierperiode legt die Granularität fest, in der Messwerte erfasst werden müssen.
Abrechnungszeitraum	Der Zeitraum für den ein Messwertsatz für die Abrechnung ermittelt werden muss.
Letztverbraucherkennung	Die eindeutige Kennung des Letztverbrauchers, der die angefallenen Daten einsehen darf.
Zugriffsberechtigungen	Zugriffsberechtigungen, 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 23: Regelwerkparameter für TAF3

4.2.2.3.3 Vom Regelwerk für externe Marktteilnehmer bereitzustellender Messwertsatz

- Für jede Laststufe: kumulierter Energiemenge zum Ende des Abrechnungszeitraums.
- Tarifwechselliste (ohne Zählerstände z.B. für Bilanzierung)

4.2.2.3.4 Für den jeweiligen Letztverbraucher an der HAN-Schnittstelle bereitzustellende Daten

- Alle Parameter des Regelwerks
- Die aktuellen Zählerstände und die kumulierte Energie je Tarifstufe, sowie Differenzbeträge zum Ende des letzten Abrechnungszeitraums (mindestens 15-minutengenau für Strom und 60-minutengenau für Gas)
- Die Momentanleistung (mindestens 15-minutengenau für Strom und 60-minutengenau für Gas)
- Die Zählerstände und Stände der Tarifstufen zum Ende eines jeden Abrechnungszeitraumes innerhalb des letzten Jahres
- Die Messwertliste (Tarifwechselliste mit Zählerständen und den zugehörigen abgeleiteten Registern)
- Alle an externe Marktteilnehmer versendete Daten

1759 ## 4.2.2.4 TAF4: Verbrauchsvariable Tarife

1760 ### 4.2.2.4.1 Beschreibung

1761 Verbrauchsvariable Tarife ermöglichen es, verbrauchte Energiemengen in Verbrauchsstufen einzu-
1762 teilen. Verbrauchsstufen haben dabei festgelegte Mengenkontingente. Sind die Kontingente einer
1763 Stufe überschritten, so wird die nächste Stufe aktiviert. Schwellenwerte legen die entsprechenden
1764 Kontingente der Stufen fest.

1765 Das SMGW erfasst den Zählerstand des Zählers (oder der Zähler) im Takt einer Registrierperiode
1766 und erzeugt zu den folgenden Zeitpunkten ein Ereignis in der zugehörigen Messwertliste:

1767 • Abrechnungszeitraum beginnt/endet
1768 • Kontingent einer Verbrauchsstufe ist überschritten (Wechsel der Verbrauchsstufe)

1769 Eine beispielhafte Messwertliste ist in Tabelle 24 angegeben.

Zeitstempel	***Grund***[14]	***Zählerstand in kWh***	***…***
01.01.2013 0:00:00h	Abrechnungszeitraum beginnt/endet	456	…
20.01.2013 12:30:00h	Verbrauchsstufe 1 aufgebraucht	556	…
31.01.2013 11:15:00h	Verbrauchsstufe 2 aufgebraucht	606	…
01.02.2013 0:00:00h	Abrechnungszeitraum beginnt/endet	608	…
…	…	…	…

1770 *Tabelle 24: Beispiel einer Messwertliste bei einem verbrauchsvariablen Tarif mit 2 Verbrauchsstufen (100kWh,*
1771 *150kWh) und einem Zähler*

1772 Zähler und Messgrößen werden über die Geräte-IDs der Zähler und die OBIS-Kennzahlen der zu
1773 erfassenden Messgrößen ausgewählt. Für den Anwendungsfall sind nur Zähler zu verwenden, die
1774 nur den Verbrauch oder nur die Einspeisung messen. Das SMGW erzeugt einen Eintrag im eich-
1775 technischen Log, für den Fall, dass der Zähler Messwerte nicht in der Frequenz der parametrisierten
1776 Abtastrate liefern kann.

1777 Zu definierten Versandzeitpunkten werden die Einträge der Messwertliste im Abrechnungszeitraum
1778 dann an berechtigte Marktteilnehmer versendet. Über Zugriffsberechtigungen wird geregelt, wel-
1779 cher Marktteilnehmer berechtigt ist.

1780 Das SMGW muss die in diesem Anwendungsfall zu versendenden Daten vor der Inhaltsdatenver-
1781 schlüsselung mit einer zusätzlichen Signatur versehen (siehe Kapitel 3.2.4.4).

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

Der Letztverbraucher ist berechtigt die aktuellen und bereits versendeten Messwerte über die HAN-Schnittstelle einzusehen (vgl. Kapitel 3.4.2.1). Über eine Letztverbraucherkennung ist der Tarif mit dem Letztverbraucher verknüpft.

Ein Gültigkeitszeitraum legt fest, ab welchen Zeitpunkt das Regelwerk in Betrieb gehen soll und zu welchem Zeitpunkt es den Betrieb wieder einstellen soll.

Hinweis: 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.

4.2.2.4.2 Notwendige Parameter für das Regelwerk

Parameter	***Beschreibung***
Geräte-IDs der Zähler	Die eindeutigen Bezeichner der Zähler.
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 des Zählpunktes.
Registrierperiode	Die Registrierperiode legt die Granularität fest, in der Messwerte vom SMGW ausgewertet werden müssen.
Definition der Verbrauchsstufen	Definiert die verschiedenen Verbrauchsstufen, deren Kontingente sowie die zugehörigen OBIS-Kennzahlen. Hier wird auch definiert, welche Tarifstufe zum Zeitpunkt der Aktivierung des Regelwerks gültig ist.
Abrechnungszeitraum	Der Zeitraum für den ein Messwertsatz für die Abrechnung ermittelt werden muss.
Letztverbraucherkennung	Die eindeutige Kennung des Letztverbrauchers, der die angefallenen Daten einsehen darf.
Zugriffsberechtigungen	Zugriffsberechtigungen, 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 25: Regelwerkparameter für TAF4

4.2.2.4.3 Vom Regelwerk für externe Marktteilnehmer bereitzustellender Messwertsatz

- Zählerstand (bzw. Summe der Zählerstände bei mehreren Zählern) zum Ende des Abrechnungszeitraums.
- Messwertliste ohne Zählerstände

4.2.2.4.4 Für den jeweiligen Letztverbraucher an der HAN-Schnittstelle bereitzustellende Daten

- Alle Parameter des Regelwerks
- Die aktuellen Zählerstände und Stände der Tarifstufen, sowie Differenzbeträge zum Ende des letzten Abrechnungszeitraums (mindestens 15-minutengenau für Strom und 60-minutengenau für Gas)
- Die aktuellen verbleibenden Kontingente der Tarifstufen
- Die Zählerstände und Stände der Tarifstufen zum Ende eines jeden Abrechnungszeitraumes innerhalb des letzten Jahres
- Die Messwertliste
- Alle an externe Marktteilnehmer versendete Daten

4.2.2.5 TAF5: Ereignisvariable Tarife

4.2.2.5.1 Beschreibung

Dieser Anwendungsfall erlaubt die Modellierung von Tarifen, die mehrere Tarifstufen vorsehen zwischen denen bei Eintritt von bestimmten Ereignissen gewechselt werden kann. Die Ereignisse sind dabei nicht unbedingt SMGW-interne Ereignisse, sondern können auch durch externe Marktteilnehmer aus dem WAN oder CLS aus dem HAN hervorgerufen werden.

Hierzu werden mehrere Tarifstufen definiert, an die jeweils Bedingungen geknüpft sind. Zu jedem Zeitpunkt ist jeweils nur eine Tarifstufe pro Anwendungsfall aktiv. Für jede Tarifstufe wird vom SMGW die Energiemenge kumuliert, die anfällt, während die Tarifstufe aktiv ist. Die gesamte Energiemenge innerhalb des Abrechnungszeitraumes wird so auf mehrere Tarifstufen verteilt.

Der Wechsel der Tarifstufen wird über den Eintritt von Ereignissen gesteuert. Dazu legt die Parametrierung fest, welche Ereignisse zu einem Wechsel in eine bestimmte Tarifstufe führen.

Findet ein Tarifwechsel statt, so erfasst das SMGW die Zählerstände von einem oder mehreren Zählern, erzeugt einen Eintrag in der Messwertliste (s. Kapitel 4.3.3) und kumuliert die am Zähler (oder den Zählern) zwischen den letzten beiden Umschaltungen angefallene Energiemenge zu der zuletzt gültigen Tarifstufe (Beispiel für ereignisvariablen Tarif mit drei Tarifstufen s. Abbildung 25).

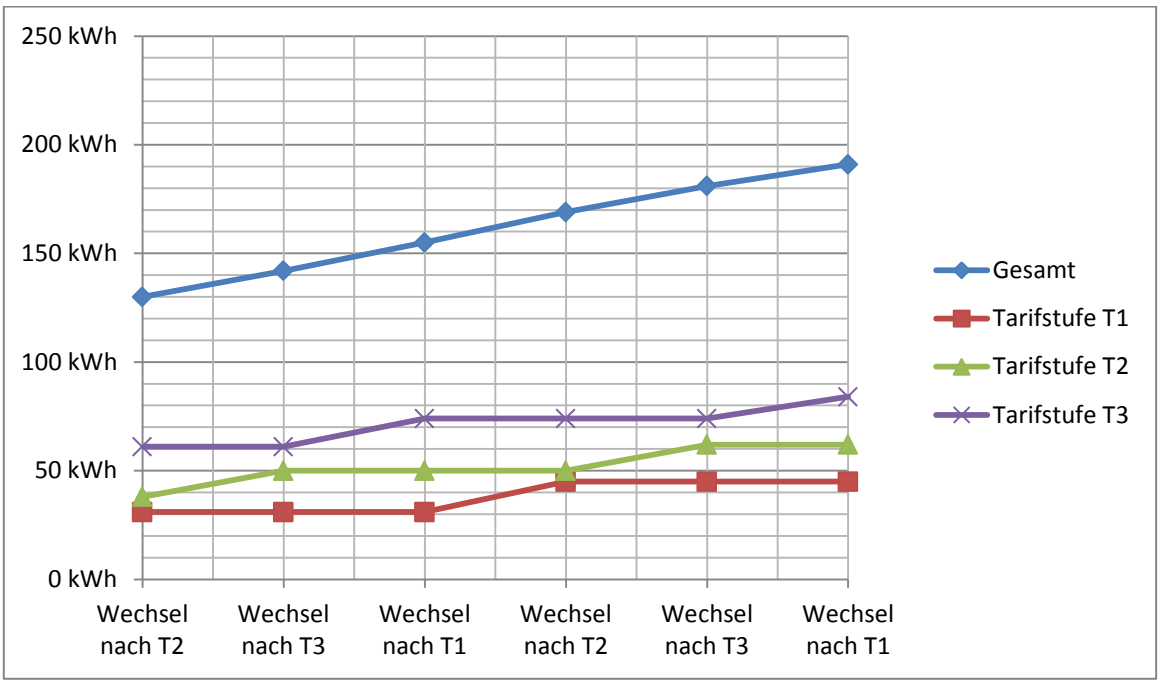

Abbildung 25: Beispiel für einen ereignisvariablen Tarif mit drei Tarifstufen und einem Zähler

Zur Bilanzierung wird die Tarifwechselliste benötigt, um die tarifierten Energiemengen tarifrichtig auf die zugehörigen Zeitabschnitte verteilen zu können. Diese kann bei ereignisgesteuerten Tarifen nur im Gateway erzeugt und daraus versendet werden.

Die als Minimum vom SMGW zu unterstützten Ereignisse sind:

- Tarifumschaltanweisungen zum Wechseln von Tarifstufen, die vom SMGW-Admin im Auftrag von autorisierten externen Marktteilnehmern aus dem WAN versendet werden

Darüber hinaus können weitere Ereignisse unterstützt werden.

Alle Tarifumschaltanweisungen, die an das SMGW versendet werden, müssen eine Bedingung beinhalten, die Auskunft darüber gibt, unter welchen Umständen die Tarifumschaltanweisung nicht mehr ausgewertet wird. Diese Bedingung muss vom SMGW vor dem Wechsel der Tarifstufen geprüft werden. Darf die Tarifumschaltanweisung aufgrund dieser Prüfung nicht mehr ausgeführt werden, so wird das gesendete Ereignis verworfen und der SMGW-Admin darüber in Kenntnis gesetzt. Die jeweiligen Bedingungen sind im Rahmen der Konfiguration der Ereignisse für Tarifstufen zu hinterlegen.

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

Zu definierten Versandzeitpunkten werden die Zählerstände der Tarifstufen dann an berechtigte Marktteilnehmer versendet. Zusätzlich kann die Liste der Tarifwechselzeitpunkte an berechtigte Marktteilnehmer versendet werden. Über Zugriffsberechtigungen wird geregelt, welcher Marktteilnehmer berechtigt ist.

Das SMGW muss die in diesem Anwendungsfall zu versendenden Daten vor der Inhaltsdatenverschlüsselung mit einer zusätzlichen Signatur versehen (siehe Kapitel 3.2.4.4).

Der Letztverbraucher ist berechtigt die aktuellen und bereits versendeten Messwerte über die HAN-Schnittstelle einzusehen (vgl. Kapitel 3.4.2.1). Über eine Letztverbraucherkennung ist der Tarif mit dem Letztverbraucher verknüpft.

Ein Gültigkeitszeitraum legt fest, ab welchen Zeitpunkt das Regelwerk in Betrieb gehen soll und zu welchem Zeitpunkt es den Betrieb wieder einstellen soll.

Hinweis: Der Anwendungsfall ermöglicht neben der Erfassung von ereignisvariablen Verbräuchen analog auch die Erfassung von ereignisvariablen Einspeisungen. In diesem Fall liefert der Zähler Messwerte für eingespeiste Energiemengen anstatt für verbrauchte Energiemengen. Weiterhin können Zähler für verbrauchte und eingespeiste Energiemengen auch zusammen veranlagt werden.

4.2.2.5.2 Notwendige Parameter für das Regelwerk

Parameter	***Beschreibung***
Geräte-IDs der Zähler	Die eindeutigen Bezeichner der Zähler.
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 des Zählpunktes.
Definition der Tarifstufen	Definiert die verschiedenen Tarifstufen sowie die zugehörigen OBIS-Kennzahlen. Hier wird auch definiert, welche Tarifstufe zum Zeitpunkt der Aktivierung des Regelwerks gültig ist.
Konfiguration der Ereignisse für Tarifstufen	Konfiguration, die festlegt, welche Ereignisse zu einem Wechsel in eine bestimmte Tarifstufe führen.
Abrechnungszeitraum	Der Zeitraum für den ein Messwertsatz für die Abrechnung ermittelt werden muss.
Letztverbraucherkennung	Die eindeutige Kennung des Letztverbrauchers, der die angefallenen Daten einsehen darf.
Zugriffsberechtigungen	Zugriffsberechtigungen, 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 26: Regelwerkparameter für TAF5

4.2.2.5.3 Vom Regelwerk für externe Marktteilnehmer bereitzustellender Messwertsatz

- Für jede Tarifstufe: kumulierter Zählerstand (oder Summe der kumulierten Zählerstände) zum Ende des Abrechnungszeitraums.
- Bei Bedarf: Tarifwechselliste (ohne Zählerstände z.B. für Bilanzierung)

4.2.2.5.4 Für den jeweiligen Letztverbraucher an der HAN-Schnittstelle bereitzustellende Daten

- Alle Parameter des Regelwerks
- Die aktuellen Zählerstände und die kumulierte Energie je Tarifstufe, sowie Differenzbeträge zum Ende des letzten Abrechnungszeitraums (mindestens 15-minutengenau für Strom und 60-minutengenau für Gas)
- Die Zählerstände und Stände der Tarifstufen zum Ende eines jeden Abrechnungszeitraumes innerhalb des letzten Jahres
- Die Messwertliste (Tarifwechselliste mit Zählerständen und den zugehörigen abgeleiteten Registern)
- Alle an externe Marktteilnehmer versendete Daten

4.2.2.6 TAF6: Abruf von Messwerten im Bedarfsfall

4.2.2.6.1 Beschreibung

Dieser Anwendungsfall erlaubt den Abruf von Messwerten in nicht planbaren Situationen, wie

- Ablesung bei Auszug und Einzug eines Letztverbrauchers,
- Ablesung bei Lieferantenwechsel und
- Ablesung bei Wechsel in den Grundversorgungstarif.

Der Anwendungsfall ist nicht im Regelbetrieb zu verwenden, sondern lediglich in begründeten Ausnahmefällen.

Um rückwirkend Ablesungen zu einem konkreten Stichtag zu ermöglichen, muss das SMGW tagesgenaue Zählerstände vorhalten. Dies geschieht automatisch für jeden am SMGW angeschlossenen Zähler und für jedes im SMGW vorhandene abgeleitete Register. Somit ist dieser Anwendungsfall immer im Hintergrund aktiv. Die Daten dürfen jedoch nur in begründeten Ausnahmefällen abgerufen werden.

Das SMGW erfasst hierzu täglich zum Beginn des abrechnungstechnischen Kalendertages den aktuellen Zählerstand des Zählers und erzeugt einen entsprechenden Eintrag in der zugehörigen Messwertliste. Messwerte, die älter als 6 Wochen sind, werden aus der Liste gelöscht.

Der SMGW-Admin kann im Auftrag eines Marktteilnehmers, der durch den Letztverbraucher berechtigt wurde, den Abruf von Messwerten im besonderen Bedarfsfall durchführen. Der SMGW-Admin gibt die angefragten Messwerte dann zu einem Stichtag an den Marktteilnehmer weiter.

Das SMGW muss die in diesem Anwendungsfall zu versendenden Daten vor der Inhaltsdatenverschlüsselung mit einer zusätzlichen Signatur versehen (siehe Kapitel 3.2.4.4).

Der Letztverbraucher ist berechtigt die aktuellen und bereits versendeten Messwerte über die HAN-Schnittstelle einzusehen (vgl. Kapitel 3.4.2.1). Der jeweilige Letztverbraucher wird über die Letztverbraucherkennung identifiziert, die dem Zähler zugeordnet sein muss.

Hinweis: Der Grund der jeweiligen Ablesung muss für den Letztverbraucher transparent und nachvollziehbar sein. Die Ablesung bei Bedarf ist nur im Sonderfall vorgesehen.

4.2.2.6.2 Notwendige Parameter für das Regelwerk

Parameter	***Beschreibung***
Geräte-IDs der Zähler	Die eindeutigen Bezeichner der Zähler.
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 des Zählpunktes.
Beginn des abrechnungstechnischen Kalendertages	Die Uhrzeit, zu der ein abrechnungstechnischer Kalendertag beginnt.
Letztverbraucherkennung	Die eindeutige Kennung des Letztverbrauchers, der die angefallenen Daten einsehen darf.

Tabelle 27: Regelwerkparameter für TAF6

4.2.2.6.3 Vom Regelwerk für externe Marktteilnehmer bereitzustellender Messwertsatz

Tagesgenaue Zählerstände und Stände der abgeleiteten Register zum angefragten Zeitpunkt innerhalb der letzten 6 Wochen.

4.2.2.6.4 Für den jeweiligen Letztverbraucher an der HAN-Schnittstelle bereitzustellende Daten

- Alle Parameter des Regelwerks
- Die tagesgenauen Zählerstände seiner eigenen Zähler in den letzten 6 Wochen
- Die tagesgenauen Stände der ihm zugeordneten abgeleiteten Register in den letzten 6 Wochen
- Die Zeitpunkte zu denen der SMGW-Admin Messwerte abgerufen hat

4.2.2.7 TAF7: Zählerstandsgangmessung

4.2.2.7.1 Beschreibung

Dieser Anwendungsfall erlaubt die Erfassung und Versendung von Zählerstandsgängen. Über diesen Anwendungsfall ist unter anderem die zentrale Tarifierung außerhalb des SMGW möglich.

Das SMGW erfasst die Zählerstände im Takt der Registrierperiode und erzeugt einen Eintrag in der zugehörigen Messwertliste.

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

Zu definierten Versandzeitpunkten werden die Messwertsätze dann an berechtigte Marktteilnehmer versendet. Über Zugriffsberechtigungen wird geregelt, welcher Marktteilnehmer berechtigt ist.

Das SMGW muss die in diesem Anwendungsfall zu versendenden Daten vor der Inhaltsdatenverschlüsselung mit einer zusätzlichen Signatur versehen (siehe Kapitel 3.2.4.4).

Der Letztverbraucher ist berechtigt die aktuellen und bereits versendeten Messwerte über die HAN-Schnittstelle einzusehen (vgl. Kapitel 3.4.2.1). Über eine Letztverbraucherkennung ist der Tarif mit dem Letztverbraucher verknüpft.

Ein Gültigkeitszeitraum legt fest, ab welchen Zeitpunkt das Regelwerk in Betrieb gehen soll und zu welchem Zeitpunkt es den Betrieb wieder einstellen soll.

Hinweis: 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.

4.2.2.7.2 Notwendige Parameter für das Regelwerk

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 des Zählpunktes.
Registrierperiode	Der zeitliche Abstand zwischen zwei aufeinanderfolgenden Messwerterfassungen für den Zählerstandsgang.
Abrechnungszeitraum	Der Zeitraum für den der Zählerstandsgang jeweils ermittelt werden soll.
Letztverbraucherkennung	Die eindeutige Kennung des Letztverbrauchers, der die angefallenen Daten einsehen darf.
Zugriffsberechtigungen	Zugriffsberechtigungen, 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 28: Regelwerkparameter für TAF7

4.2.2.7.3 Vom Regelwerk für externe Marktteilnehmer bereitzustellender Messwertsatz

Der Zählerstandsgang für den Abrechnungszeitraum.

4.2.2.7.4 Für den jeweiligen Letztverbraucher an der HAN-Schnittstelle bereitzustellende Daten

- Alle Parameter des Regelwerks
- Die aktuellen Zählerstände (mindestens 15-minutengenau für Strom und 60-minutengenau für Gas)
- Die Messwertliste
- Alle an externe Marktteilnehmer versendete Daten

4.2.2.8 TAF8: Erfassung von Extremwerten für Leistung

4.2.2.8.1 Beschreibung

Dieser Anwendungsfall erlaubt die Erhebung von Maximal- bzw. Minimalleistungswerten, die innerhalb eines Abrechnungszeitraums anfallen.

Hierzu erfasst das SMGW im Takt der Registrierungsperiode den aktuellen Zählerstand des Zählers (oder mehrerer Zähler) und speichert diesen in der Messwertliste ab. Das SMGW berechnet auf Basis von zwei aufeinanderfolgenden Zählerständen den Leistungsmittelwert der Registrierperiode.

Nach Ablauf jedes Abrechnungszeitraums bestimmt das SMGW die n niedrigsten und die m höchsten Werte der Leistungsmittelwerte im Abrechnungszeitraum. Die Anzahlen m und n der jeweiligen Extremwerte werden über die Parametrierung festgelegt. Bei mehreren Zählern wird jeweils zunächst die Summe über die verschiedenen Leistungswerte je Registrierperiode gebildet und dann aus den Summen die Extremwerte ausgewählt.

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

Zu definierten Versandzeitpunkten werden die Extremwerte dann an berechtigte Marktteilnehmer versendet. Zusätzlich kann die Liste der Tarifwechselzeitpunkte an berechtigte Marktteilnehmer versendet werden. Über Zugriffsberechtigungen wird geregelt, welcher Marktteilnehmer berechtigt ist.

Das SMGW muss die in diesem Anwendungsfall zu versendenden Daten vor der Inhaltsdatenverschlüsselung mit einer zusätzlichen Signatur versehen (siehe Kapitel 3.2.4.4).

Der Letztverbraucher ist berechtigt die aktuellen und bereits versendeten Messwerte über die HAN-Schnittstelle einzusehen (vgl. Kapitel 3.4.2.1). Über eine Letztverbraucherkennung ist der Tarif mit dem Letztverbraucher verknüpft.

Ein Gültigkeitszeitraum legt fest, ab welchen Zeitpunkt das Regelwerk in Betrieb gehen soll und zu welchem Zeitpunkt es den Betrieb wieder einstellen soll.

Hinweis: 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.

4.2.2.8.2 Notwendige Parameter für das Regelwerk

Parameter	***Beschreibung***
Geräte-IDs der Zähler	Die eindeutigen Bezeichner der Zähler.
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 des Zählpunktes.
Registrierperiode	Der Takt in dem Messwerte erfasst werden sollen.
Anzahl Minimalwerte n	Anzahl der Minimalwerte der Leistungsmittelwerte, die für einen Abrechnungszeitraum bestimmt werden sollen.
Anzahl Maximalwerte m	Anzahl der Maximalwerte der Leistungsmittelwerte, die für einen Abrechnungszeitraum bestimmt werden sollen.
Abrechnungszeitraum	Der Zeitraum für den ein Messwertsatz für die Abrechnung ermittelt werden muss.
Letztverbraucherkennung	Die eindeutige Kennung des Letztverbrauchers, der die angefallenen Daten einsehen darf.
Zugriffsberechtigungen	Zugriffsberechtigungen, 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.

Tabelle 29: Regelwerkparameter für TAF8

4.2.2.8.3 Vom Regelwerk für externe Marktteilnehmer bereitzustellender Messwertsatz

- Die n niedrigsten Werte der Leistungsmittelwerte eines Zählers mit den jeweiligen Zeitstempeln (oder der Summe der Leistungsmittelwerte mehrerer Zähler) im Abrechnungszeitraum
- Die m höchsten Werte der Leistungsmittelwerte eines Zählers mit den jeweiligen Zeitstempeln (oder der Summe der Leistungsmittelwerte mehrerer Zähler) im Abrechnungszeitraum

4.2.2.8.4 Für den jeweiligen Letztverbraucher an der HAN-Schnittstelle bereitzustellende Daten

- Alle Parameter des Regelwerks
- Die n niedrigsten Werte der Leistungsmittelwerte eines Zählers mit den jeweiligen Zeitstempeln (oder der Summe der Leistungsmittelwerte mehrerer Zähler) im Abrechnungszeitraum

- Die m höchsten Werte der Leistungsmittelwerte eines Zählers mit den jeweiligen Zeitstempeln (oder der Summe der Leistungsmittelwerte mehrerer Zähler) im Abrechnungszeitraum
- Die Messwertliste
- Alle an externe Marktteilnehmer versendete Daten

4.2.3 Anwendungsfälle für steuerbare Anlagen

4.2.3.1 TAF9: Abruf der Ist-Einspeisung einer Erzeugungsanlage

4.2.3.1.1 Beschreibung

Dieser Anwendungsfall erlaubt die aktuelle Ist-Einspeiseleistung einer Erzeugungsanlage im Rahmen einer aktuell durchgeführten Energiemanagementmaßnahme auszulesen und einem berechtigten externen Marktteilnehmer zur Verfügung zu stellen.

Ein berechtigter externer Marktteilnehmer kann mit Hilfe des SMGW-Admins den Abruf der Ist-Einspeiseleistung veranlassen. Dieser muss dann nach erfolgreichem Durchführen des Wake-Up-Service die Erfassung und den Versand der aktuellen Einspeiseleistung anstoßen oder die Ereignisse konfigurieren, welche den Versand auslösen. Über Zugriffsberechtigungen wird geregelt, welcher Marktteilnehmer dazu berechtigt ist.

Das SMGW muss die in diesem Anwendungsfall zu versendenden Daten vor der Inhaltsdatenverschlüsselung mit einer zusätzlichen Signatur versehen (siehe Kapitel 3.2.4.4).

Zähler und Messgröße werden über die Geräte-ID des Zählers und die OBIS-Kennzahl der Messgröße ausgewählt.

Der Letztverbraucher ist berechtigt die aktuellen und bereits versendeten Messwerte über die HAN-Schnittstelle einzusehen (vgl. Kapitel 3.4.2.1). Der jeweilige Letztverbraucher wird über die Letztverbraucherkennung identifiziert, die dem Zähler zugeordnet sein muss.

Eine Messwertliste wird für diesen Anwendungsfall nicht angelegt. Des Weiteren darf dieser Anwendungsfall aus eichtechnischer Sicht nicht zu Abrechnungszwecken verwendet werden.

4.2.3.1.2 Notwendige Parameter für das Regelwerk

Parameter	***Beschreibung***
Geräte-ID des Zählers	Der eindeutige Bezeichner des Zählers.
OBIS-Kennzahl der zu verwendenden Messgröße	Die eindeutige Kennzahl der für den Tarif zu verwendenden Messgröße des Zählers.
Zählpunktbezeichnung	Der eindeutige Bezeichner des Zählpunktes.
Letztverbraucherkennung	Die eindeutige Kennung des Letztverbrauchers, der die angefallenen Daten einsehen darf.
Zugriffsberechtigungen	Zugriffsberechtigungen, die regeln, wer die ermittelten Daten

Parameter	*Beschreibung*
	über HAN oder WAN erhalten oder auslesen darf.

Tabelle 30: Regelwerkparameter für TAF10

4.2.3.1.3 Vom Regelwerk für externe Marktteilnehmer bereitzustellende Messwertsatz

Die jeweils aktuelle Ist-Einspeisung der Erzeugungsanlage.

4.2.3.1.4 Für den jeweiligen Letztverbraucher an der HAN-Schnittstelle bereitzustellenden Daten

- Alle Parameter des Regelwerks
- Die aktuelle Ist-Einspeisung der Erzeugungsanlage
- Alle an externe Marktteilnehmer versendete Daten

4.2.4 Anwendungsfälle für Netzzustandsdatenerhebung

4.2.4.1 TAF10: Abruf von Netzzustandsdaten

4.2.4.1.1 Beschreibung

Dieser Anwendungsfall ermöglicht die Bereitstellung von Netzzustandsdaten im SMGW oder der Statusinformationen der am Gateway angeschlossenen Zählern, die periodisch oder bei Eintritt bestimmter Ereignisse an berechtigte Marktteilnehmer versendet werden können. Der Anwendungsfall ist insbesondere vorgesehen, um den Netzbetreibern zu ermöglichen, den Zustand ihrer Netze zu beurteilen. Die Daten, die bezüglich dieses Anwendungsfalls erhoben werden, werden in der Regel pseudonymisiert versendet und sind in der Regel nicht abrechnungsrelevant. Bei entsprechender Zweckbindung kann jedoch die Pseudonymisierung deaktiviert werden.

Die als Minimum vom SMGW zu unterstützenden auslösenden Ereignisse sind:

- Veranlassung durch den SMGW-Admin.
- Ein Messwert überschreitet einen bestimmten Schwellwert.
- Ein Messwert unterschreitet einen bestimmten Schwellwert.
- Eine bestimmte Statusinformation wird vom Zähler an das SMGW gesendet. Es dürfen nur solche Statusinformationen an externe Marktteilnehmer gesendet werden, die vom SMGW interpretierbar sind.

Weitere Ereignisse können vorgesehen werden.

Zähler und Messgrößen der Netzzustandsdaten werden über die Geräte-ID des Zählers und die O-BIS-Kennzahlen der Messgrößen ausgewählt.

Bei Eintritt eines der definierten Ereignisse werden die Messwerte vom SMGW erfasst und an berechtigte Marktteilnehmer versendet. Über Zugriffsberechtigungen wird geregelt, welcher Marktteilnehmer berechtigt ist.

Bei der Pseudonymisierung der Zustandsdaten wird statt der Geräte-ID des Zählers ein Pseudonym verwendet, welches nur der SMGW-Admin kennt. Der berechtigte Markteilnehmer kann in diesem Fall den Bezug zum Zähler nicht herstellen. Soll aus berechtigten Gründen keine Psedonymisierung der Daten erfolgen, so wird weiterhin die Geräte-ID des Zählers versendet.

Der Letztverbraucher ist berechtigt die versendeten Messwerte über die HAN-Schnittstelle einzusehen (vgl. Kapitel 3.4.2.1). Der jeweilige Letztverbraucher wird über die Letztverbraucherkennung identifiziert, die dem Zähler zugeordnet sein muss.

Eine Messwertliste wird für diesen Anwendungsfall nicht angelegt.

4.2.4.1.2 Notwendige Parameter für das Regelwerk

Parameter	***Beschreibung***
Geräte-ID des Zählers	Der eindeutige Bezeichner des Zählers.
Liste von OBIS-Kennzahlen der als Netzzustandsdaten zu verwendenden Messwerte	Die eindeutigen Kennzahlen der als Netzzustandsdaten zu verwendenden Messgrößen des Zählers.
Zählpunktbezeichnung	Der eindeutige Bezeichner des Zählpunktes.
Statusinformationen (optional)	Statusinformationen der Zähler, die bei entsprechender Zweckbindung an berechtigte externe Marktteilnehmer gesendet werden können. Diese müssen vom SMGW interpretierbar sein.
Letztverbraucherkennung	Die eindeutige Kennung des Letztverbrauchers, der die angefallenen Daten einsehen darf. Hier Letztverbraucher oder EEG-Anlagenbetreiber.
Zugriffsberechtigungen	Zugriffsberechtigungen, die regeln, wer die ermittelten Daten über HAN oder WAN erhalten oder auslesen darf.
Ereignisse	Ereignisse, welche die Versendung der Daten auslösen.
Pseudonym (optional)	Pseudonym, welches bei der Versendung der ermittelten Werte anstatt der Geräte-ID des Zählers versendet werden muss. Das Pseudonym wird vom SMGW-Admin vorgegeben und kann im Bedarfsfall von diesem auch wieder auf den Zähler zurückgeführt werden. Dieser Parameter ist nur dann zu setzen, wenn eine Pseudonymisierung notwendig ist.

Tabelle 31: Regelwerkparameter für TAF10

4.2.4.1.3 Vom Regelwerk für externe Marktteilnehmer bereitzustellender Messwertsatz

Die Liste der als Netzzustandsdaten ausgewählten Messwerte.

4.2.4.1.4 Für den jeweiligen Letztverbraucher an der HAN-Schnittstelle bereitzustellende Daten

- Alle Parameter des Regelwerks

4.2.5 Informative Anwendungsfälle

Die in diesem Kapitel beschriebenen Anwendungsfälle haben informativen Charakter.

4.2.5.1 TAF11: Steuerung von unterbrechbaren Verbrauchseinrichtungen und Erzeugungsanlagen

4.2.5.1.1 Beschreibung

Dieser Anwendungsfall ermöglicht Tarife, die bei Erhalt von Steuersignalen oder anderen externen Ereignissen für unterbrechbare Verbrauchseinrichtungen oder steuerbaren Erzeugungsanlagen den Zeitpunkt des Ereignisses und die aktuellen Messwerte des Zählers (oder der Zähler) festhalten. Mit diesen Messwertsätzen kann dann beispielsweise nachgelagert bei einem externen Marktteilnehmer, der Verlust berechnet werden, der dem Letztverbraucher durch das Abschalten der Einspeisung über die Steuerung entstanden ist.

Die zu erfassenden Messwerte sind die vom Zähler gemessene Energiemenge (oder Summe der gemessenen Energiemengen bei mehreren Zählern) und die gemessene Momentanleistung des Zählers (bzw. die Summe der gemessenen Momentanleistungen bei mehreren Zählern). Jede Steuerhandlung führt zu einem Eintrag in der Messwertliste. Eine beispielhafte Messwertliste ist in Tabelle 32 angegeben.

Zeitstempel	***Grund (Ereignis)[15]***	***Zählerstand Zähler 1 in kWh***	***Leistung Zähler 1 in kWh***	***…***
02.01.2013 13:15:11h	Anlage wird auf 70% geregelt.	123	5	…
20.01.2013 15:30:43h	Anlage wird auf 50% geregelt.	145	2	…
31.01.2013 18:15:10h	Anlage wird auf 30% geregelt.	167	6	…
01.02.2013 22:11:00h	Anlage wird abgeschaltet (0%).	189	8	…
01.02.2013 23:21:20h	Anlage wird auf 30% geregelt.	189	2	…
…	…	…		…

Tabelle 32: Beispiel für eine Messwertliste im Fall einer steuerbaren Erzeugungsanlage mit einem Zähler

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

Das SMGW muss die in diesem Anwendungsfall zu versendenden Daten vor der Inhaltsdatenverschlüsselung mit einer zusätzlichen Signatur versehen (siehe Kapitel 3.2.4.4).

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

Der Letztverbraucher als Betreiber der Anlage ist berechtigt die aktuellen und bereits versendeten Messwerte über die HAN-Schnittstelle einzusehen (vgl. Kapitel 3.4.2.1). Über eine Letztverbrauchererkennung ist der Tarif mit dem Letztverbraucher verknüpft.

4.2.5.1.2 Notwendige Parameter für das Regelwerk

Parameter	***Beschreibung***
Geräte-IDs der Zähler	Die eindeutigen Bezeichner der Zähler.
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 des Zählpunktes.
Steuersignale	Die Liste der im Regelwerk zu berücksichtigenden externen Ereignisse.
Letztverbraucherkennung	Die eindeutige Kennung des Letztverbrauchers, der die angefallenen Daten einsehen darf.
Zugriffsberechtigungen	Zugriffsberechtigungen, 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.

Tabelle 33: Regelwerkparameter *für TAF9*

4.2.5.1.3 Vom Regelwerk für externe Marktteilnehmer bereitzustellender Messwertsatz

- Das für die Steuerung relevante externe Ereignis
- Die aktuelle Einspeisemenge
- Die Momentanleistung zum Zeitpunkt der Steuerung inklusive des zugehörigen Zeitstempels

4.2.5.1.4 Für den jeweiligen Letztverbraucher bereitzustellender Messwertsatz

- Alle Parameter des Regelwerks
- Die Messwertliste
- Alle an externe Marktteilnehmer versendete Daten

4.2.5.2 TAF12: Prepaid Tarif

4.2.5.2.1 Beschreibung

Dieser Anwendungsfall ermöglicht einen Prepaid-Tarif. Dabei handelt es sich um einen Tarif, bei dem ein bestimmter Betrag bei einem externen Marktteilnehmer (z.B. Energielieferanten) entrichtet und dafür eine bestimmte Energiemenge zur Verfügung gestellt wird. Hierzu konfiguriert der SMGW Administrator die verfügbare Energiemenge als Parameter des zugehörigen Auswertungsprofils (vgl. Kapitel 4.4.3).

Zusätzlich zu der verfügbaren Energiemenge wird vom SMGW Administrator auch immer ein Startzeitpunkt als Parameter an das SMGW übermittelt. Damit kann das SMGW feststellen, wann die verfügbare Energiemenge aufgebraucht wird. Zu diesem Zwecke erfasst das SMGW von einem oder mehreren relevanten angeschlossenen Zählern mindestens im 15-Minuten-Takt für Strom und 60-Minuten-Takt für Gas jeweils einen Zählerstand.[16] Die Zählerstände werden in der zugeordneten Messwertliste eingetragen. Anhand der Zählerstände berechnet das SMGW bei jedem Eintreffen eines neuen Messwertes die noch verfügbare Energiemenge.

Ist die verfügbare Energiemenge verbraucht, so sendet das SMGW nach Ablauf des Toleranzzeitraums ein Signal an einen Stromunterbrecher.

Es muss eine Benachrichtigung an den EMT erfolgen, wenn die verfügbare Energiemenge einen konfigurierten Schwellwert unterschritten hat bzw. die Energiemenge verbraucht ist. Über Zugriffsberechtigungen wird geregelt, welcher Marktteilnehmer berechtigt ist.

Es muss eine Benachrichtigung an den Letztverbraucher erfolgen, wenn die verfügbare Energiemenge einen konfigurierten Schwellwert unterschritten hat bzw. die Energiemenge verbraucht ist. Die Benachrichtigungen müssen im Letztverbraucher-Log registriert werden.

Der Anwendungsfall betrachtet nur eine Tarifstufe. Es ist dabei möglich, die Zählerstände mehrerer Zähler eines Letztverbrauchers zu addieren und als Gesamtverbrauch dem Letztverbraucher zur Verfügung zu stellen.

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

Der Letztverbraucher ist berechtigt die aktuellen und falls vorhanden die bereits versendeten Messwerte über die HAN-Schnittstelle einzusehen (vgl. Kapitel 3.4.2.1). Über eine Letztverbraucherkennung ist der Tarif mit dem Letztverbraucher verknüpft.

Ein Gültigkeitszeitraum legt fest, ab welchen Zeitpunkt das Regelwerk in Betrieb gehen soll und zu welchem Zeitpunkt es den Betrieb wieder einstellen soll.

4.2.5.2.2 Notwendige Parameter für das Regelwerk

Parameter	**Beschreibung**
Geräte-IDs der Zähler	Die eindeutigen Bezeichner der Zähler.
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 des Zählpunktes.
Verfügbare Energiemenge	Die verfügbare Energiemenge in kWh oder m^3
Toleranzzeitraum	Die Länge des Zeitraums in dem der Letztverbraucher nach

[16] Kleinere Zeiträume können gewählt werden, solange die Anforderungen aus Kapitel 3.2.6 erfüllt werden.

Parameter	Beschreibung
	Verbrauch der verfügbaren Energiemenge noch Energie beziehen kann.
Schwellwert	Definierter Schwellwert der verfügbaren Energiemenge in kWh oder m³.
Startzeitpunkt	Der Zeitpunkt, ab dem die verfügbare Energiemenge freigeschaltet wird.
Geräte-IDs der Unterbrecher	Die eindeutigen Bezeichner der Unterbrecher, die zum Zeitpunkt des Verbrauches der verfügbaren Energiemenge, ein Signal vom SMGW erhalten.
Letztverbraucherkennung	Die eindeutige Kennung des Letztverbrauchers, der die angefallenen Daten einsehen darf.
Zugriffsberechtigungen	Zugriffsberechtigungen, 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. Hier kann auch festgelegt werden, dass der berechtigte EMT sofort zu informieren ist, wenn die verfügbare Energiemenge verbraucht ist.
Gültigkeitszeitraum	Der Zeitraum für den das Regelwerk im SMGW verwendet werden soll.

Tabelle 34: Regelwerkparameter für TAF12

4.2.5.2.3 Vom Regelwerk für externe Marktteilnehmer bereitzustellende Messwertsatz

- Zeitpunkt, an dem die verfügbare Energiemenge den konfigurierten Schwellwert unterschreitet
- Zeitpunkt, an dem die verfügbare Energiemenge verbraucht ist
- Zeitpunkt, an dem der Toleranzzeitraum abgelaufen ist

4.2.5.2.4 Für den jeweiligen Letztverbraucher zu visualisierende Daten

- Alle Parameter des Regelwerks
- Noch verfügbare Energiemenge in kWh oder m^3 (muss mindestens alle 15 Minuten für Strom und alle 60 Minuten für Gas aktualisiert werden)
- Die aktuellen Zählerstände und deren Summe (müssen mindestens alle 15 Minuten für Strom und alle 60 Minuten für Gas aktualisiert werden)
- Die Zählerstände und deren Summe zum Zeitpunkt jeder Parametrierung der verfügbaren Energiemenge im Auswertungsprofil durch den SMGW Administrator innerhalb des letzten Jahres
- Die Messwertliste (mindestens 15-minutengenau für Strom und 60-minutengenau für Gas)
- Zeitpunkt, an dem die verfügbare Energiemenge den konfigurierten Schwellwert unterschreitet

- Zeitpunkt, an dem die verfügbare Energiemenge verbraucht ist
- Der noch verbleibende Toleranzzeitraum in Minuten
- Alle an externe Marktteilnehmer versendete Daten

4.2.5.3 TAF13: Bereitstellung von Messwertsätzen zur Visualisierung für den Letztverbraucher über die WAN-Schnittstelle

Dieser Anwendungsfall kann eine Alternative zur lokalen Visualisierung darstellen. Dabei stellt die Messwertverarbeitung die anwendungsfallspezifischen Messwertsätze (nach TAF1 – TAF12) an der WAN-Schnittstelle bereit, um Letztverbraucher-spezifische Daten zum Zwecke der Visualisierung für den Letztverbraucher zur Verfügung zu stellen.

4.2.6 Übersicht der Anwendungsfälle

Anwendungsfall	*Auslöser im Regelwerk*
TAF1: Datensparsame Tarife	Internes Ereignis: Zeitpunkt
TAF7: Zählerstandsgangmessung	
TAF8: Erfassung von Extremwerten	
TAF2: Zeitvariable Tarife	
TAF3: Lastvariable Tarife	Internes Ereignis: Grenzwert
TAF4: Verbrauchsvariable Tarife	
TAF12: Prepaid Tarif (informativ)	
TAF5: Ereignisvariable Tarife	Internes oder externes Ereignis
TAF10: Abruf von Netzzustandsdaten	
TAF11: Steuerung von unterbrechbaren Verbrauchseinrichtunge und Erzeugungsanlagen (informativ)	Externes Ereignis
TAF9: Abruf der Ist-Einspeisung	
TAF6: Ablesung von Messwerten im Bedarfsfall	

Tabelle 35: Zuordnung der Anwendungsfälle zu den jeweiligen Auslösern im Regelwerk

4.3 Messwertverarbeitung mit Regelwerken

4.3.1 Konzeptübersicht

Dieses Kapitel hat informativen Charakter.

Das Konzept der Messwertverarbeitung ist in Abbildung 26 dargestellt.

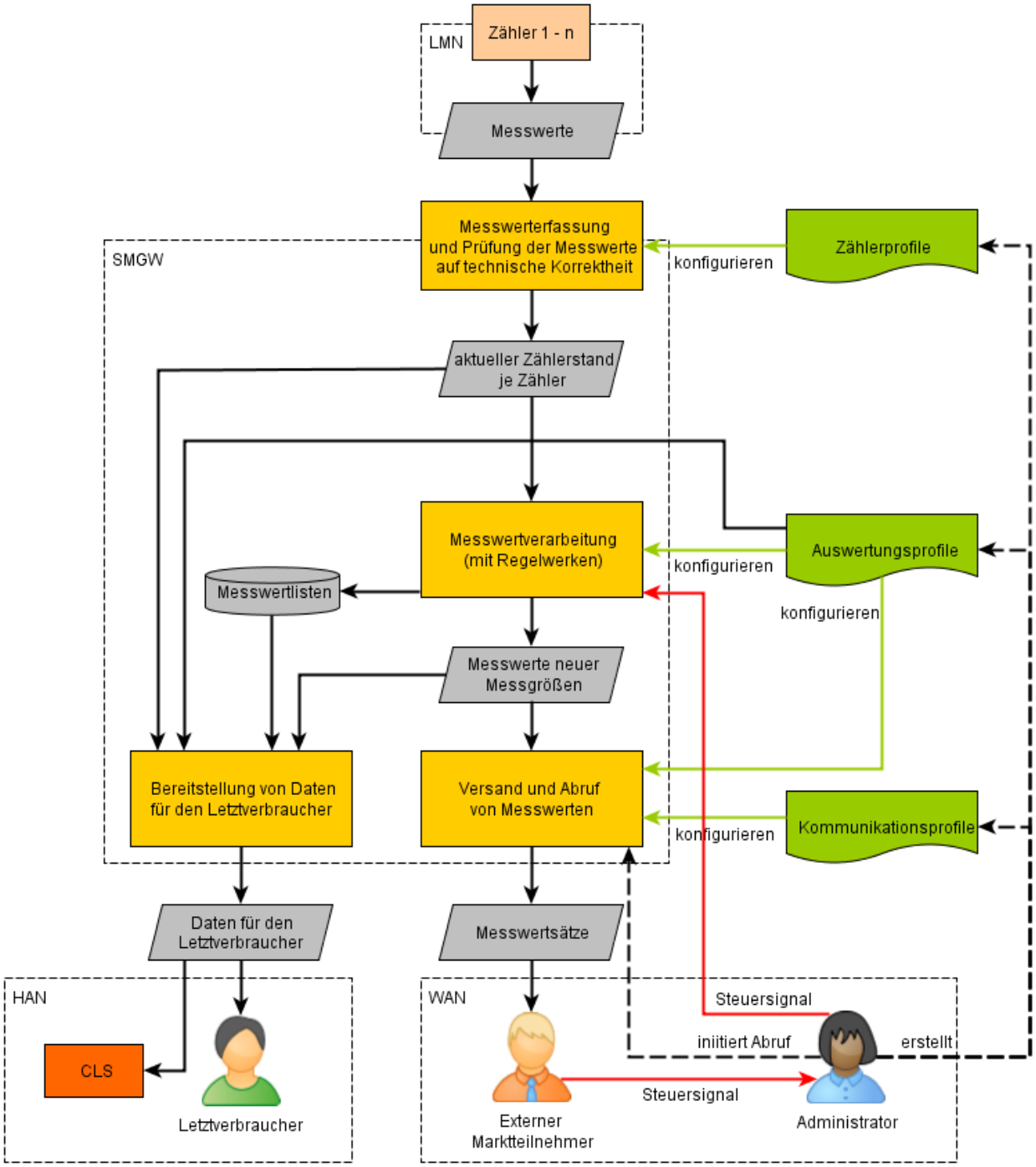

Abbildung 26: Übersicht der Messwertverarbeitung (maßgeblich für AF1-AF10)

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.

Regelwerke verarbeiten die erfassten originären Messwerte und speichern die Ergebnisse in abgeleiteten Registern bzw. in abgeleiteten Wertelisten, die dann für den Versand an externe Marktteilnehmer vorgehalten werden. Abgeleitete Register bzw. Wertelisten werden vom SMGW für die Modellierung der verschiedenen Tarifstufen aus den Anwendungsfällen (s. Kapitel 4.2) verwendet. Das SMGW kann mehrere Regelwerke parallel betreiben, um Messwertverarbeitungen auch für mehrere Letztverbraucher 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 Letztverbraucher seine Abrechnungen anhand der originären Messwerte der Zähler nachvollziehen kann. Jeder Letztverbraucher kann dazu die ihm zugeordneten Messwertlisten und die Werte der abgeleiteten Register / Wertelisten über die Anzeigeeinheit (IF_GW_CON) einsehen (s. Kapitel 3.4.2.1).

Die Konfiguration sämtlicher Teilaspekte der Messwerterfassung und -verarbeitung obliegt dem SMGW-Admin. Regelwerke werden über Auswertungsprofile konfiguriert, welche die Parameter für die verschiedenen Anwendungsfälle aus Kapitel 4.2 festlegen. Diese legen auch die Berechtigungen fest, die den externen Markteilnehmer im WAN oder aber CLS im HAN Zugriff auf die abgeleiteten Register ermöglichen. Der Letztverbraucher 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 SMGW-Admin eingebrachte Kommunikationsprofile legen fest, über welchen TLS-Kanal Messwerte an externe Markteilnehmer im WAN versendet werden.

4.3.2 Messwerterfassung

Das SMGW muss Zählerstände von mehreren angeschlossenen Zählern erfassen können. Jeder Zähler muss über seine Geräte-ID im SMGW eindeutig identifizierbar und adressierbar sein. Es dürfen nur untarifierte Messwerte verwendet werden. Demnach müssen für die Erfassung von Strom ausschließlich die OBIS Value Group A=1 und E=0 verwendet werden. Für die Erfassung von Gas müssen ausschließlich die OBIS Value Group A=7, B=0, C=3 oder C=6, D=0 oder D=6 und E=0 verwendet werden. Bei dem Empfang von Zählerständen muss das SMGW die Sicherung der Kommunikation gemäß Kapitel 3.3.5.2 sicherstellen und das jeweilige Fachprotokoll nach Kapitel 3.3.5.1 auswerten. Die Konfiguration dazu muss vom SMGW-Admin durch Zählerprofile (siehe Kapitel 4.4.2) eingebracht werden können.

Das SMGW **MUSS** zu jedem angeschlossenen Zähler aktuelle Zählerstände der relevanten gemessenen Messgrößen vorhalten. Der SMGW-Admin **MUSS** dazu konfigurieren können, welche Messgrößen des Zählers relevant sind und in Form von aktuellen Zählerständen im SMGW abgebildet werden müssen. Zu jedem Zählerstand **MÜSSEN** der Zeitstempel des Eingangs, die Statuszusatzinformationen des Zählers und das vom SMGW gebildete Statuswort abgelegt werden (siehe Kapitel 4.3.4 und Kapitel 4.3.5). An externe Marktteilnehmer dürfen jedoch keine Daten versendet werden, die nicht vom SMGW inhaltlich interpretiert werden können.

Das SMGW **MUSS** Messwerte im 15-Minutentakt für Strom und 60-Minutentakt für Gas erfassen können und mindestens in diesem Takt aktuelle Zählerstände von den Zählern vorhalten können. Da unter Umständen nicht alle Zähler in der Lage sind, Messwerte in diesen Auflösungen zu liefern, **MUSS** das SMGW anhand der Parameter des Zählerprofils prüfen, ob ein Zähler in der Lage ist die für den jeweiligen Anwendungsfall geforderte Granularität der Messwerte zu gewährleisten.

Das SMGW **MUSS** bei der Erfassung von Messwerten technische Korrektheitsprüfungen durchführen, um zu entscheiden, ob ein Messwert gültig ist. Details zur Umsetzung der Korrektheitsprüfungen sind in Kapitel 4.3.4 zu finden.

Für die Identifizierung von Messgrößen der Zähler **MÜSSEN** OBIS-Kennzahlen verwendet werden [IEC 62056-6-1].

Jedem Zähler **MUSS** der Letztverbraucher zugeordnet werden, dessen Verbrauch oder Einspeisung er misst.

Das SMGW **MUSS** Messwerte in der Granularität erfassen, wie sie für das jeweilige Regelwerk, welches den Anwendungsfall abbildet, notwendig sind (Datensparsamkeit und Zweckbindung).

4.3.3 Messwertverarbeitung

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

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

Die abgeleiteten Register **MÜSSEN** für die Abbildung der verschiedenen Tarifstufen der Anwendungsfälle (s. Kapitel 4.2) verwendet werden. Die abgeleiteten Wertelisten **MÜSSEN** für die Abbildung von Zählerstandsgängen, den Messwertlisten und der anderen auf Listen basierenden Messwertsätzen der Anwendungsfälle verwendet werden.

Das SMGW **MUSS** Tarifumschaltanweisungen, die vom SMGW-Admin aus dem WAN an das SMGW versendet werden, zeitstempeln und aufzeichnen können. Das SMGW **MUSS** Tarifumschaltanweisungen in den Regelwerken berücksichtigen können, um Tarifumschaltungen bei diesen Ereignissen zu ermöglichen (z.B. Ereignisvariable Tarife, siehe Kapitel 4.2.2.5).

Das SMGW **MUSS** abgeleitete Register oder Wertelisten dem Letztverbraucher zuordnen, für den die Auswertungen vorgenommen werden. Die aktuellen und die bereits versendeten Werte der abgeleiteten Register oder Wertelisten müssen von dem zugehörigen Letztverbrauchers eingesehen werden können.

Die Inhalte abgeleiteter Register und Wertelisten **MÜSSEN** auch bei einem Zählerwechsel erhalten und weiter verwendet werden können.

Die Parametrierung des Regelwerks über Auswertungsprofile **MUSS** alleinig durch dem SMGW-Admin eingespielt werden können (s.a. Kapitel 3.2.2, Anwendungsfall WAF1).

Die Parametrierung **MUSS** auch festlegen, wer Zugriff auf die Messwertsätze haben darf, die vom Regelwerk für externe Marktteilnehmer für den jeweiligen Anwendungsfall bereitgestellt werden. Hierfür **MUSS** eine Zugriffskontrolle vorgesehen werden, die festlegt, welcher externe Marktteilnehmer welche abgeleiteten Register oder Wertelisten Inhalte erhalten darf. Zusätzlich muss festgelegt werden, welcher Letztverbraucher Zugriff auf diese Daten erhält.

Das SMGW **KANN** die Messwertverarbeitung des SMGW so konstruieren, dass sie in eichpflichtige und in nicht eichpflichtige Teile aufgeteilt wird.

Die eichrechtlich relevanten Funktionen im SMGW **MÜSSEN** in einem oder mehreren separaten Modulen implementiert werden, welche separat versioniert werden. So kann bei einer Softwareänderung zwischen einer Änderung an eichrechtlich relevanten Softwareteilen und anderen nicht eichrechtlich relevanten Softwareteilen unterschieden werden.

Auch für die Identifizierung der Messgrößen in den abgeleiteten Registern und Wertelisten **MÜSSEN** OBIS-Kennzahlen verwendet werden [IEC 62056-6-1]. Die OBIS-Kennzahlen der abgeleiteten Register bzw. der Wertelisten **MÜSSEN** dem SMGW und dem jeweiligen Auswertungsprofil zugeordnet werden. Die Zuordnung sichert die Eindeutigkeit. Zusätzliche Identifikatoren sind zulässig. Damit sind Überschneidungen bei der Identifizierung von Messgrößen zwischen originären Messgrößen der Zähler und abgeleiteten Registern und Wertelisten ausgeschlossen.

Jeder originäre Messwert eines Zählers, der im Regelwerk für die Messwertverarbeitung verwendet wird und im eichrechtlichen Sinne für die Bildung neuer abrechnungsrelevanten Messgrößen herangezogen wird, **MUSS** zusätzlich in eine Messwertliste abgelegt werden. Zum Messwert **MÜSSEN** außerdem eine laufende Nummer, der Zeitstempel der Erfassung, die Statuszusatzinformationen der technischen Korrektheitsprüfungen und der Grund für die Erfassung in der Messwertliste abgelegt werden.

Alle aus originären Messwerten berechneten Messwerte **MÜSSEN** mir drei Nachkommastellen im SMGW vorgehalten werden. Es gelten die folgenden Rundungsregeln:

- Ist die Ziffer an der ersten wegfallenden Dezimalstelle eine 0,1,2,3 oder 4, dann wird abgerundet.
- Ist die Ziffer an der ersten wegfallenden Dezimalstelle eine 5,6,7,8 oder 9, dann wird aufgerundet.

Das SMGW **MUSS** Einträge in den Messwertlisten solange aufbewahren, bis das Ende des jeweiligen Abrechnungszeitraums zuzüglich mindestens 3 Monate überschritten 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 eichrechtlich relevant sind. Die Menge der eichrechtlich relevanten Statusinformationen, ist in Tabelle 36 angegeben.[17]

Enthält der vom SMGW empfange Messwert eine solche Statusinformation, so muss das SMGW die in Tabelle 36 beschriebenen Aktionen durchführen. Der empfangene Messwert darf nicht zur Bildung oder Veränderung von abgeleiteten Registern durch das SMGW verwendet werden.

Statuswort des Zählers	***Bedeutung***	***Aktion durch das SMGW***
Fataler Fehler	Gerät muss ausgetauscht werden	Push-Meldung an den SMGW-Admin und an autorisierte externe Marktteilnehmer

Tabelle 36: 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. Alle notwendigen Prüfungen, die mindestens vom SMGW durchgeführt werden **MÜSSEN**, sind in Tabelle 37 beschrieben. Zusätzlich **KÖNNEN** weitere Prüfungen durchgeführt werden.

Verläuft eine in Tabelle 37 aufgeführte Prüfung negativ, so **MUSS** dies als Statusinformation des SMGW festgehalten werden und die entsprechenden Aktionen durch das SMGW ausgeführt werden (vgl. Tabelle 37). Der empfangene Messwert darf nicht zur Bildung oder Veränderung von abgeleiteten Registern durch das SMGW verwendet werden.

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 SMGW-Admin
Ist die Zeit der Systemuhr korrekt?	Zeitinformation ist ungültig	Push-Meldung an den SMGW-Admin

Tabelle 37: Technische Korrektheitsprüfungen, die vom SMGW durchzuführen sind

[17] Es dürfen nur solche Zähler für die Bildung und Änderung von abgeleiteten Registern verwendet werden, welche in der Lage sind, die in Tabelle 36 aufgeführten Statusinformationen zu senden.

Liegen nach Durchführung aller in diesem Kapitel beschriebenen Prüfungen Statusinformationen gemäß Tabelle 36 oder Tabelle 37 vor, so **MUSS** das SMGW unter Verwendung dieser Informationen ein allgemeines Statuswort bilden. Dieses sowie die Statusinformationen gemäß Tabelle 36 oder Tabelle 37 (diese liegen weiterhin als Rohdaten vor) werden im System-Log und im eichtechnischem Log gespeichert. Außerdem werden die Statusinformationen gemäß Tabelle 36 oder Tabelle 37 sowie das allgemeine Statuswort zusammen mit dem Zählerstand im Letztverbraucher-Log gespeichert und falls in Tabelle 36 oder Tabelle 37 gefordert an externe Marktteilnehmer versendet. Dabei darf das SMGW den Zählerstand nicht an den SMGW-Admin versenden oder im System-Log oder im eichtechnischen Log speichern.

4.3.4.2 Weitere Prüfungen und Versand von Statusinformationen

Dieses Kapitel hat informativen Charakter.

Zusätzlich zu den in Kapitel 4.3.4.1 aufgeführten Prüfungen können auch anwendungsfallspezifische Prüfverfahren angewandt werden. Dazu können die jeweiligen Prüfkriterien im Auswertungsprofil des zugehörigen Anwendungsfalls hinterlegt werden (vgl. 4.4.3).[18] In diesem Fall muss das Auswertungsprofil auch eine Beschreibung enthalten, wie im Fall einer negativ verlaufenden Prüfung zu verfahren ist. Dabei muss sichergestellt werden, dass keine Informationen, die nicht vom SMGW interpretiert werden können an externe Marktteilnehmer versendet werden dürfen.

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 (vgl. 4.2.4.1) an autorisierte externe Teilnehmer übermittelt werden. Dabei muss sichergestellt werden, dass alle an externe Marktteilnehmer gesendeten Statusinformationen vom SMGW interpretiert werden können.

4.3.5 Zeitstempelung von Messwertsätzen

Die Zeitpunkte der Erfassung von Zählerständen **MÜSSEN** im SMGW auf Basis einer im SMGW verbauten Uhr bestimmt werden.

Wird von einem Zähler in 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. Nach erfolgreicher Korrektheitsprüfung (vgl. Kapitel 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.

[18] 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.

4.3.6 Kommunikation und Versand von Messwertsätzen

Konfigurationen für die Kommunikation mit Teilnehmern im HAN und WAN **MÜSSEN** durch den SMGW-Admin mittels Kommunikationsprofilen nach Kapitel 4.4.4 eingespielt werden können.

Beim Versand von Messwerten **MÜSSEN** immer die folgenden Informationen versendet werden:

- Geräte-ID des Zählers (oder Pseudonym)
- Zeitstempel der versendeten Messwertsätze und Zeitstempel der Versendung
- OBIS-Kennzahlen des Messwertsatzes
- Messwertsatz
- Ggf. Statusinformation (vergleiche dazu Kapitel 4.3.4)

Das SMGW **MUSS** die oben genannten Informationen auch im Letztverbraucher-Log des jeweiligen Letztverbrauchers hinterlegen.

Die zu übertragenden Daten **MÜSSEN** wie in Kapitel 3.2.4 beschrieben abgebildet werden.

4.3.7 Bereitstellung von Daten für den Letztverbraucher

Unabhängig von der Messwerterfassung für Abrechnungszwecke oder Statusdatenerhebung **MUSS** das SMGW die empfangenen Messwerte auch für die Visualisierung auf der Anzeigeeinheit des Letztverbrauchers bereitstellen. Entsprechende Vorgaben sind je Anwendungsfall in Kapitel 4.2 genannt.

Der Letztverbraucher **MUSS** einsehen können, wann welche Messwerte aus welchem Grund an externe Marktteilnehmer versendet worden sind. Entsprechende Ereignisse **MÜSSEN** in seinem Letztverbraucher-Log hinterlegt werden.

4.4 Konfigurationsprofile

4.4.1 Einleitung

Die Konfiguration der Zähleranbindung, Messwerterfassung, -verarbeitung und –versand sowie der Kommunikation zu externen Marktteilnehmern im WAN wird über Konfigurationsprofile festgelegt, die vom SMGW-Admin in das SMGW eingespielt werden.

Die Konfigurationsprofile **MÜSSEN** in XML-Format abgebildet sein. Vor dem Einstellen der Konfigurationsprofile **MUSS** der SMGW-Admin diese auf Plausibilität prüfen. Des Weiteren **MUSS** das SMGW eine Schemaprüfung durchführen.

Abbildung 27 stellt die Beziehungen zwischen den verschiedenen Profilen dar.

Abbildung 27: 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. Zählerprofile **MÜSSEN** die folgenden Parameter beinhalten:

Parameter	***Datentyp / Wertebereich[19]***	***Beschreibung***
Geräte-ID	Octet String	Der eindeutige Bezeichner des Zählers.
Kommunikationsszenario gemäß Kapitel 3.3.3	Einer aus: LKS1 LKS2	Legt das Kommunikationsszenario fest (siehe Kapitel 3.3.3
Kommunikationstyp	TLS Symmetrisch	Legt fest, ob TLS oder das symmetrische kryptographische Verfahren für die Sicherung der Kommunikation verwendet werden soll.
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 oder Key-ID im Sicherheitsmodul und Zertifikate	Das Schlüsselmaterial für die Absicherung der Kommunikation mit dem Zähler. Im Fall des symmetrischen Verfahrens ist das notwendige Schlüsselmaterial ein symmetrischer Schlüssel. Im Fall von TLS muss der private Schlüssel im Sicherheitsmodul ausgewählt werden, der für die Authentifizierung gegenüber dem Zähler gewählt werden muss, das entsprechende Zertifikat für diesen Schlüssel und das Zertifikat des Zählers.
Intervall	Sekunden	Das Intervall, in dem Messwerte vom Zähler empfangen bzw. ausgelesen werden müssen und in dem der im SMGW vorgehaltene aktuelle Zählerstand aktualisiert werden muss.

[19] Die hier dargestellten Datentypen und Wertebereiche besitzen informativen Charakter.

Parameter	*Datentyp / Wertebereich*[19]	*Beschreibung*
Saldierend	Ja/Nein	Legt fest, ob der Zähler ein saldierender Zähler ist und seine Zählerstände sowohl größer als auch kleiner werden können.
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.
Wandlerfaktoren		Beträgt bei direkt anzuschließenden Zählern immer 1. Bei Verwendung von Wandlerzählern kann der Faktor abweichend sein.

Tabelle 38: Parameter von Zählerprofilen

Das SMGW **KANN** weitere Parameter für Zählerprofile unterstützen.

Zählerprofile werden über die Geräte-Ids der Zähler in Auswertungsprofilen referenziert.

Die Datenstruktur der Zählerprofile **MUSS** wie in Kapitel 3.2.4.1 beschrieben abgebildet werden.

4.4.3 Auswertungsprofile

Ein Auswertungsprofil parametrisiert ein Regelwerk, für einen konkreten Anwendungsfall. Auswertungsprofile **MÜSSEN** die folgenden Parameter beinhalten:

Parameter	*Datentyp / Wertebereich*[20]	*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 Kapitel 4.2)
Alle für den jeweiligen Anwendungsfall notwendigen Parameter	Siehe entsprechendes Unterkapitel in Kapitel 4.2.	Siehe entsprechendes Unterkapitel in Kapitel 4.2.
Optional die vom SMGW durchzuführenden Prüfungen der Messwerte		Siehe Kapitel 4.3.4.2
Zugeordnete Kommunikationsprofile	1..n Bezeichner	Die Bezeichner referenzieren die Kommunikationsprofile, die für den Versand von verarbeiteten Messwerten an externe Marktteilnehmer verwendet werden.

Tabelle 39: Durch Auswertungsprofile festzulegende Parameter eines Regelwerks

Das SMGW **KANN** weitere Parameter für Auswertungsprofile unterstützen.

[20] Die hier dargestellten Datentypen und Wertebereiche besitzen informativen Charakter.

Die Datenstruktur der Auswertungsprofile **MUSS** wie in Kapitel 3.2.4.1 beschrieben abgebildet werden.

Auswertungsprofile **MÜSSEN** vom SMGW-Admin eingespielt werden können. Vor der Aktivierung des Auswertungsprofils **MUSS** das SMGW die folgenden Punkte sicherstellen:

- Die anhand der Geräte-ID referenzierten Zähler sind durch Zählerprofile konfiguriert.
- Die referenzierten Zähler müssen in der Lage sein, die im Auswertungsprofil geforderte Granularität der Messwert zu gewährleisten.
- Die im Auswertungsprofil angegebenen OBIS-Kennzahlen für Messgrößen sind auch im jeweiligen Zählerprofil hinterlegt.
- Alle referenzierten Kommunikationsprofile sind im SMGW vorhanden.
- Die verschiedenen Tarifstufen und Messwertlisten, die nach den Anwendungsfällen ausgewertet werden sollen, **MÜSSEN** im SMGW als abgeleitete Register oder abgeleitete Wertelisten eingerichtet werden, sofern diese Objekte noch nicht existieren.

Wird eine der genannten Prüfung nicht bestanden, so **DARF** das Auswertungsprofil **NICHT** aktiviert werden und eine entsprechender Eintrag **MUSS** ins System-Log des SMGW geschrieben werden.

Nach der Aktivierung ist das Regelwerk konfiguriert und die Messwertverarbeitung **MUSS** beginnen.

4.4.4 Kommunikationsprofile für die WAN-Kommunikation

Ein WAN-Kommunikationsprofil legt die Parameter für die Kommunikation zu einem externen Marktteilnehmer im WAN oder dem SMGW-Admin fest.

WAN-Kommunikationsprofile **MÜSSEN** zumindest die folgenden Parameter beinhalten:

Parameter	***Datentyp / Wertebereich[21]***	***Beschreibung***
Bezeichner	Alphanummerisch	Der im SMGW eindeutige Bezeichner des Kommunikationsprofils.
Name	Text	Ein verständlicher Name für das Kommunikationsprofil.
Kommunikationsszenario gemäß Kapitel 3.2.3	MANAGEMENT ADMIN-SERVICE INFO-REPORT	Legt das Kommunikationsszenario fest (siehe Kapitel 3.2.3)
Rolle des Kommunikationspartners	Einer aus: SMGW-Admin EMT	Legt die Rolle des Kommunikationspartners fest.

[21] Die hier dargestellten Datentypen und Wertebereiche besitzen informativen Charakter.

Parameter	***Datentyp / Wertebereich[21]***	***Beschreibung***
Adresse(n) des externen Marktteilnehmers oder des SMGW-Admins	1..n URI	Legt eine oder mehrere Adressen fest, an denen der externe Markteilnehmer erreichbar ist und zu der ein TLS-Kanal vom SMGW aufgebaut werden muss.
Keepalive	Ja/Nein	Legt fest, ob der TLS-Kanal dauerhaft aufgehalten werden soll, auch wenn die Aktion, die zum Aufbau geführt hat, nicht mehr gegenwärtig 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	0..n	Anzahl der TLS-Kanalaufbauversuche im Fehlerfall. Führen alle Versuche zu einem Fehler, so muss das Ereignis im System-Log eingetragen werden.
Wartezeit im Fehlerfall	0..n Sekunden	Die Wartezeit zwischen Kanalaufbauversuchen.
Wartezeit im Leerlauf	0..n Sekunden	Nach Ablauf der Zeit im Leerlauf, wird der TLS-Kanal wieder abgebaut. Der Wert 0 deaktiviert den Abbau im Leerlauf.
Maximale Sitzungslänge	0..172800 Sekunden	Die maximale Zeit, die ein TLS-Kanal aufgehalten werden soll. Ein Wert größer als 48h darf vom SMGW nicht akzeptiert werden.
Zertifikat des externen Markteilnehmers für die TLS-Authentifizierung	Zertifikat	Das Zertifikat des externen Marktteilnehmers für die TLS-Authentifizierung des externen Markteilnehmers durch das SMGW.
Zertifikat des externen Markteilnehmers für die Signierung der Inhaltsdaten	Zertifikat	Das Zertifikat des externen Marktteilnehmers für Signierung von Inhaltsdaten, die vom externen Markteilnehmer durchgeführt werden muss.
Zertifikat des externen Markteilnehmers für den Schlüsseltransport	Zertifikat	Das Zertifikat des externen Marktteilnehmers für den Schlüsseltransport von symmetrischen Schlüsseln für die Verschlüsselung von Inhaltsdaten, die vom SMGW durchgeführt werden muss.
Zertifikat des SMGW für die TLS-Authentifizierung	Zertifikat	Ein Zertifikat des SMGW für die TLS-Authentifizierung durch den externen Markteilnehmer.
Privater Schlüssel des SMGW für die TLS-Authentifizierung	Key-ID des Sicherheitsmoduls	Eine Referenz auf einen Schlüssel im Sicherheitsmodul, der für die TLS-Authentifizierung des SMGW verwendet werden muss.
Zertifikat des SMGW für die Signierung von Inhaltsdaten	Zertifikat	Ein Zertifikat des SMGW das für die Signierung von Inhaltsdaten durch das SMGW verwendet werden muss.

Parameter	***Datentyp / Wertebereich[21]***	***Beschreibung***
Privater Schlüssel des SMGW für die Signierung von Inhaltsdaten	Key-ID des Sicherheitsmoduls	Eine Referenz auf einen Schlüssel im Sicherheitsmodul, der für die Signierung von Inhaltsdaten durch das SMGW verwendet werden muss.
Zertifikat des SMGW für den Schlüsseltransport	Zertifikat	Ein Zertifikat des SMGW, das für den Schlüsseltransport von symmetrischen Schlüsseln für die Entschlüsselung von Inhaltsdaten im SMGW verwendet werden muss.
Privater Schlüssel des SMGW für den Schlüsseltransport	Key-ID des Sicherheitsmoduls	Eine Referenz auf einen Schlüssel im Sicherheitsmodul, der für den Schlüsseltransport von symmetrischen Schlüsseln für die Entschlüsselung von Inhaltsdaten im SMGW verwendet werden muss.

Tabelle 40: Durch WAN-Kommunikationsprofile festzulegende Parameter

Das SMGW **KANN** weitere Parameter für WAN-Kommunikationsprofile unterstützen.

WAN-Kommunikationsprofile **MÜSSEN** nur vom SMGW-Admin eingespielt werden können. Vor der Aktivierung der Kommunikationsprofile **MUSS** das SMGW die folgenden Punkte sicherstellen:

- Es **MUSS** mindestens ein WAN-Kommunikationsprofil mit der Rolle „SMGW-Admin“ und den Kommunikationsszenarien MANAGEMENT und ADMIN-SERVICE aktiviert sein.
- Die referenzierten Key-Ids existieren im Sicherheitsmodul.
- Der Rolle EMT **MUSS** in den WAN-Kommunikationsprofilen ausschließlich das Kommunikationsszenario INFO-REPORT zugeordnet werden.
- Der Rolle SMGW-Admin **MÜSSEN** in den WAN-Kommunikationsprofilen ausschließlich die Kommunikationsszenarien MANAGEMENT und ADMIN-SERVICE zugeordnet werden.

Zusätzlich **MUSS** das SMGW vor der Deaktivierung eines Kommunikationsprofils prüfen, dass kein Auswertungsprofil auf das zu deaktivierende Kommunikationsprofil verweist.

Wird eine der genannten Prüfungen nicht bestanden, so **DARF** das Auswertungsprofil **NICHT** aktiviert werden und eine entsprechender Eintrag **MUSS** ins System-Log des SMGW geschrieben werden.

Die Datenstruktur der Kommunikationsprofile **MUSS** wie in Kapitel 3.2.4.2.1 beschrieben abgebildet werden.

4.5 Anforderungen an Zugriffsberechtigungen

4.5.1 Einleitung

Dieses Kapitel klärt allgemeine Anforderungen an die Zugriffsberechtigungen der verschiedenen Nutzer des SMGW.

4.5.2 Generelle Zugriffsbeschränkungen

- Es **DARF KEIN** geheimes Schlüsselmaterial im SMGW ausgelesen werden können.
- 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 Administrator

- Der SMGW-Admin **MUSS** alleinig die Berechtigungen haben, die Konfiguration des SMGW vorzunehmen. Dies betrifft insbesondere:
  - Konfiguration für Messwerterfassung, Messwertverarbeitung und Versand von Messwerten und anderen Informationen an weitere Marktteilnehmer
  - Einspielung von Firmware-Updates nach Überprüfung der Authentizität der Firmware
  - Konfiguration für die Festlegung welche externen Marktteilnehmer mit dem SMGW kommunizieren dürfen und welche Informationen diese über externe Schnittstellen erhalten dürfen
  - Konfiguration des Sicherheitsmoduls
  - Konfiguration des Zertifikatsmaterials im SMGW
- Der Administrator **DARF** Messwertlisten **NICHT** einsehen können.
- Der Administrator **MUSS** das Eichtechnische Log und das System-Log einsehen können.
- Der Administrator **DARF** das Eichtechnische Log und das System-Log **NICHT** ändern können.
- Der Administrator **DARF** die Letztverbraucher-Logs der Letztverbrauchers **NICHT** einsehen oder ändern können.
- Der Administrator **MUSS** als Einziger die Berechtigung haben, das SMGW über den Wake-Up-Service aufzuwecken.

4.5.4 Service-Techniker

- Der Service-Techniker **MUSS** ausschließlich die folgenden Informationen an der Diagnoseschnittstelle des SMGW einsehen können:
  - Das System-Log des SMGW.
  - Diagnose-Informationen gemäß Anwendungsfall HAF2 in Kapitel 3.4.2.

4.5.5 Letztverbraucher

- Ein Letztverbraucher **MUSS** über die HAN-Schnittstelle des SMGW Informationen einsehen können, die ihn betreffen:
  - Konfiguration der Zähler, Auswertungsprofile, Kommunikationsprofile, Zählerstände und Messwertlisten die für den Letztverbraucher relevant sind.
  - Eigene aktuelle und vergangene Verbrauchs- und/oder Einspeisewerte (s.a. Kapitel 3.4.2.1)
  - das eigene Letztverbraucher-Log
- Der Letztverbraucher **DARF** Daten, die nur andere Letztverbraucher betreffen, **NICHT** einsehen können.

4.5.6 Externe Marktteilnehmer

- Ein externer Marktteilnehmer **MUSS** ausschließlich Informationen vom SMGW erhalten dürfen, die durch Auswerteprofile vom SMGW-Admin festgelegt worden sind.
- Externe Marktteilnehmer **DÜRFEN KEINEN** direkten Zugriff auf Zähler im LMN haben.
- Externe Marktteilnehmer **DÜRFEN KEINEN** direkten Zugriff auf Messwertlisten haben, sofern der jeweilige Anwendungsfall (s. Kapitel 4.2) dies nicht rechtfertigt.

5 Weitere Funktionale Anforderungen

5.1 Zusammenspiel SMGW und Sicherheitsmodul

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

5.1.1 Nutzung des Sicherheitsmoduls beim TLS-Handshake

Die Vorgaben an die Implementierung der kryptographischen Primitive von TLS sind in [BSI TR-03109-3] definiert und **MÜSSEN** befolgt werden. Dabei **MUSS** das SMGW mit einem Sicherheitsmodul zusammenarbeiten, das gemäß [SM_PP] zertifiziert wurde.

Beim Aufbau des TLS-Kanals (Handshake) **MUSS** das SMGW sein Sicherheitsmodul einsetzen, wie in Abbildung 28 und Abbildung 29 beispielhaft dargestellt. Folgende Funktionen des Sicherheitsmoduls **MÜSSEN** verwendet werden:

- Generierung von Zufallszahlen für TLS-Kommando ClientHello
- Schlüsselaushandlung des TLS pre-master secrets gemäß Elliptic Curve Diffie-Hellman
- Signaturerzeugung und –prüfung für Authentifizierung

Das SMGW ist verantwortlich für die Generierung des *master secrets* und **MUSS** dazu das ausgehandelte *pre-master secret* verwenden.

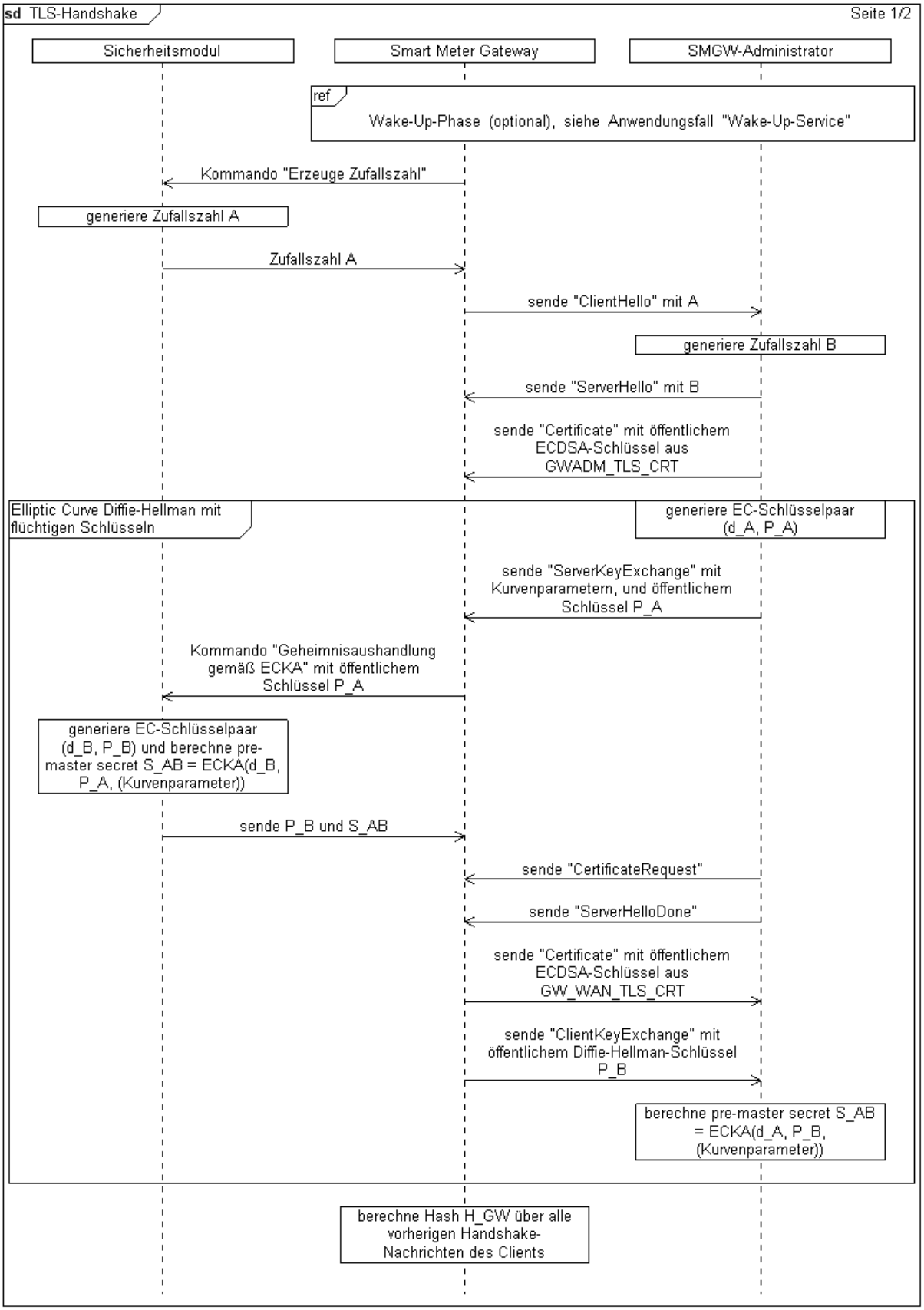

Abbildung 28: Sequenzdiagramm Interaktion zwischen Gateway und Sicherheitsmodul beim TLS-Handshake 1/2

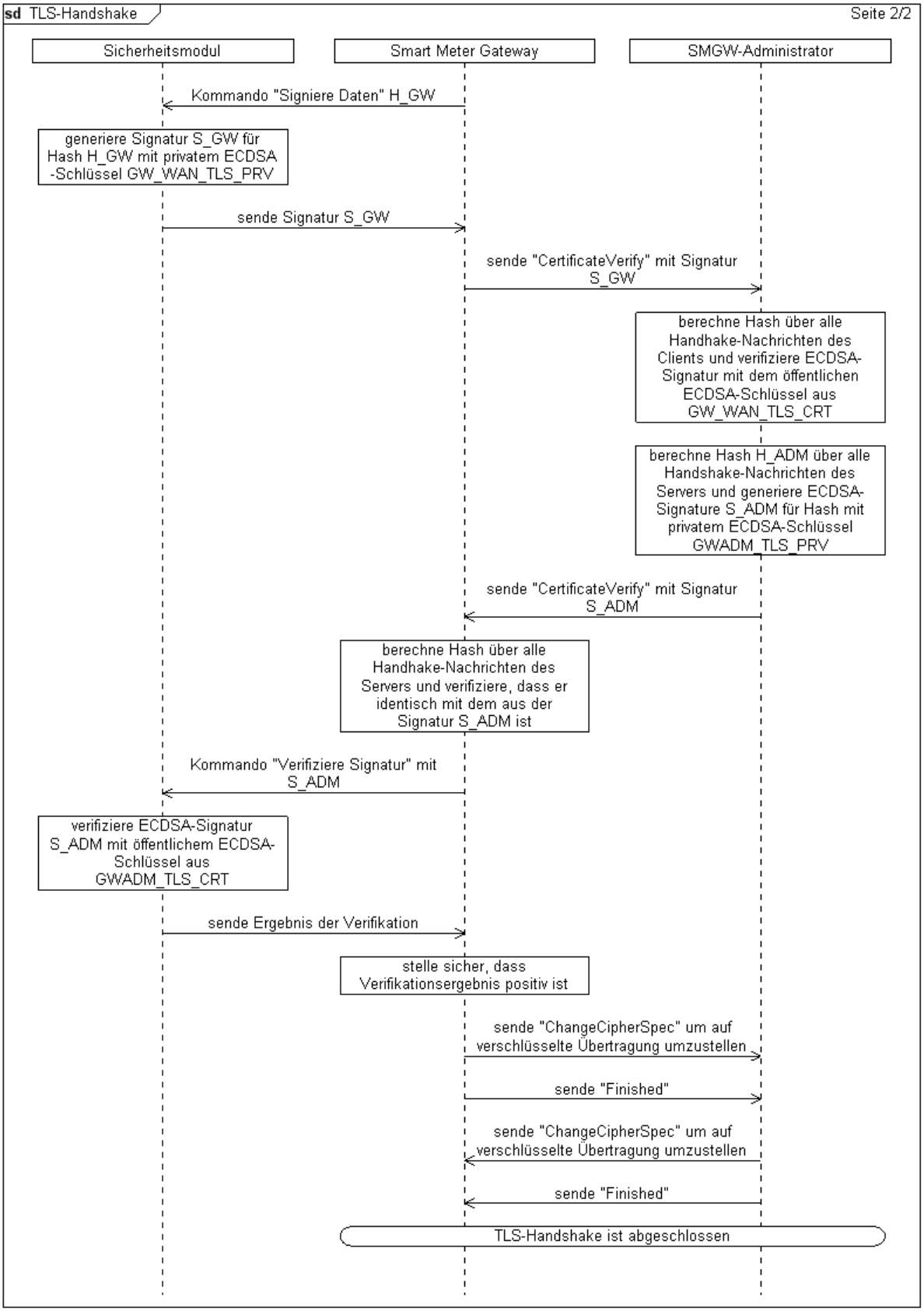

Abbildung 29: Sequenzdiagramm Interaktion zwischen Gateway und Sicherheitsmodul beim TLS-Handshake 2/2

Die Reihenfolge der TLS-Kommandos beim TLS-Handshake **KANN** von der in den Abbildungen gezeigten Reihenfolge eventuell abweichen. Die Abbildungen sind diesbezüglich lediglich exemplarisch und informativ zu verstehen. Ausschlaggebend ist die Anforderung in [BSI 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** Inhaltsdaten einer WAN Kommunikation (Netzzustandsdaten, Abrechnungsdaten, Administrationsdaten, Managementdaten, …) mit einem symmetrischen Verschlüsselungsverfahren verschlüsseln.

Weiterhin **MUSS** das SMGW die verschlüsselten Inhaltsdaten mit einem MAC sichern.

Die verschlüsselten Inhaltsdaten **MÜSSEN** schließlich mit einer kryptographischen Signatur gesichert werden.

Die Schlüssel (bzw. der Schlüssel bei AES im GCM-Mode) für Inhaltsdatenverschlüsselung und MAC-Sicherung **MÜSSEN** vom Sicherheitsmodul zufällig erzeugt werden. Der Schlüssel zur Verschlüsselung dieser beiden symmetrischen Schlüssel **MUSS** dann durch einen auf elliptischen Kurven basierenden Schlüsselaustausch hergeleitet werden. Hierbei **MUSS** eine entsprechende Schlüsselableitungsfunktion (KDF) verwendet werden. Das SMGW **MUSS** hierzu die Vorgaben aus [BSI TR-03109-3] umsetzen.

Die Hash-Generierung, die symmetrische Verschlüsselung sowie die Schlüsselableitung **MÜSSEN** vom SMGW implementiert werden, während für die folgenden Funktionen das Sicherheitsmodul verwendet werden **MUSS**:

- Generierung von Zufallszahlen für symmetrische Verschlüsselung
- Schlüsselaushandlung gemäß Elliptic Curve Diffie-Hellman
- Signaturerzeugung

[BSI TR-03109-3] zeigt hierzu die zu verwendenden kryptographischen Algorithmen und Schlüssellängen auf.

Abbildung 30 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 P_B des Empfängers mit dem dazugehörigen privaten Schlüssel d_B im Besitz des Empfängers auf der WAN-Seite ist.

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

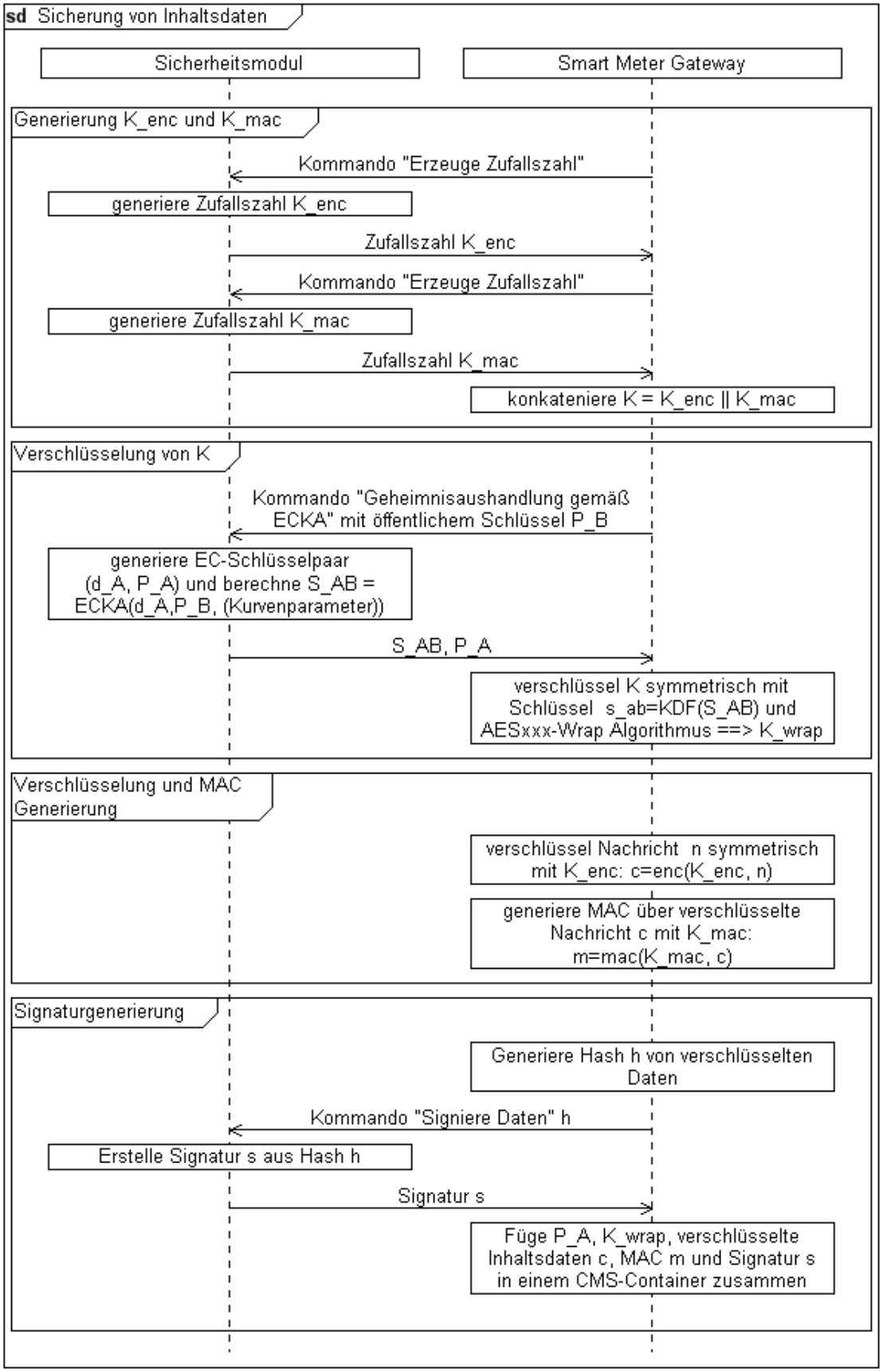

Abbildung 30: Sequenzdiagramm Interaktion zwischen Gateway und Sicherheitsmodul bei der Inhaltsdatensicherung unter Verwendung von AES-CBC-CMAC

Der kurzlebige Schlüssel P_A, 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 (Cryptographic Message Syntax) Container gemäß Kapitel 3.2.4.4 verpackt werden.

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.

Das SMGW **MUSS** gemäß Schutzprofil [GW_PP] Kapitel 4.1, Sicherheitsziel O.Log mindestens drei Klassen von Log-Informationen implementieren:

Log-Klasse	***Zugriff***	***Schnittstelle***
System-Log	lesender Zugriff durch den autorisierten SMGW Administrator	WAN Schnittstelle
System-Log	Lesender Zugriff durch den autorisierten Systemtechniker	HAN Schnittstelle (IF_GW_SRV)
Letztverbraucher-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 SMGW Administrator	WAN Schnittelle

Tabelle 41: Log-Klassen und erlaubter Zugriff

Die konkrete Implementierung der Log-Informationen **KANN** so realisiert werden, dass tatsächlich drei separate Dateien beschrieben werden. System-Log und Letztverbraucher-Log **KÖNNEN** als Ringspeicher implementiert werden, so dass bei Überlauf der älteste Log-Eintrag überschrieben wird. Dabei **MUSS** die Größe des Ringspeichers so bemessen sein, dass als Minimum die Daten der letzten 15 Monate vorgehalten werden können. Einträge im Eichtechnischen Log dürfen gemäß Schutzprofil [GW_PP] niemals gelöscht werden. Die Größe des Speichers **MUSS** entsprechend dimensioniert sein. Andere Implementierungen (z.B. als Log-Records in einer Datenbank) sind ebenfalls möglich.

Die Zugriffsbeschränkungen auf diese Log-Records **MÜSSEN** allerdings, wie in obiger Tabelle beschrieben, auf jeden Fall umgesetzt werden.

Die folgenden Informationen **MUSS** jeder Log-Eintrag beinhalten:

Merkmal	***Bedeutung***	***o/m/c***[22]
record_number	Eine eindeutige Zahl, die diesen Log-Eintrag kennzeichnet	m
datetime	Datum und Uhrzeit in UTC (Coordinated Universal Time), wann der Log-Eintrag geschrieben wurde, z.B. „2012-09-06T12:34:47“	m

[22] o: optional, m: mandatory, d.h. verpflichtend, c: conditional

Merkmal	***Bedeutung***	***o/m/c***[22]
level	Loglevel, die Einstufung der Wichtigkeit des Logeintrages • „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:“.	m
event_type	Art des aufgezeichneten Ereignisses • Auftreten eines sicherheitsrelevanten Ereignisses • Verbindungsauf- bzw. abbau zu WAN Teilnehmer • Übertragung abrechnungsrelevanter Messdaten zu WAN Teilnehmer • Übertragung nicht abrechnungsrelevanter Messdaten zu WAN Teilnehmer • Erstellen/Löschen/Bearbeiten eines Auswertungs- oder Kommunikationsprofils • Änderung der SMGW Konfiguration durch den Administrator • 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 [CCPart2V3.1]) definiert sind	m
subject_identity	Identität des Subjektes (Prozess, Anwendungskomponente, Benutzer, Profil), durch das ein Ereignis ausgelöst wurde.	o
outcome	Ergebnis, der mit dem Log-Event verbundenen Aktionen • „S“: Success Die Aktion wurde erfolgreich abgeschlossen • „F“: Failure Die Aktion konnte nicht erfolgreich durchgeführt werden. • „X:***“: eXtension Herstellerspezifisches Ergebnis, Detailangaben folgen dem „X:“.	m
message	Eine das Log-Event zusätzlich beschreibende Erklärung bzw. die Parameter des geloggten Ereignisses. Diese sind abhängig vom „event_type“.	m

Merkmal	*Bedeutung*	*o/m/c*[22]
user_identity	Die Identität des Benutzers, durch den das Ereignis ausgelöst wurde, bzw. für den die Aktion durchgeführt wurde. Bei der Übertragung von Messdaten an WAN Teilnehmer **MUSS** in diesem Feld insbesondere die Identität des Anschlussnutzers geloggt werden, dessen Daten übermittelt wurden. Die Log-Einträge im Letztverbraucher-Log **MÜSSEN** das Attribut „user_identity“ gesetzt haben. Dadurch soll gewährleistet werden, dass verschiedene Anschlussnutzer nur die für sie bestimmten Letztverbraucher-Log-Einträge in der Anzeigeeinheit dargestellt bekommen (Mandantenfähigkeit des SMGW).	o
destination	Adresse des Kommunikationspartners beim Verbindungsaufbau und Datenaustausch (z.B. URL)	o
evidence	(falls vorhanden) Signatur der übertragenen Messdaten durch das SMGW, zur Beweisbarkeit der Authentizität und des Ursprungs der übertragenen Messdaten	c

Tabelle 42: 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 SMGW Administrator wird durch entsprechende COSEM Klassen und das Transferprotokoll an der WAN Schnittstelle festgelegt.

Die Syntax der Log-Einträge des Letztverbraucher-Logs beim Auslesen durch einen berechtigten Benutzer an der HAN-Schnittstelle **MUSS** dem XML-Schema SmartMetering_Logging.xsd [XML_LOG] genügen. Darüber hinaus ist eine Anzeige in einem Webbrowser ohne Beachtung des XML Schemas zulässig.

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 Kapitel 4.5 beschrieben sind, nicht verletzt werden.

5.3.1 Obligatorische Einträge im Eichtechnischem Log

Das Eichtechnische Log dient der Registrierung von Änderungen an eichtechnisch relevanten Soft- und Firmware Anteilen sowie den Konfigurationsprofilen und den zugehörigen Parametern. Des Weiteren **MÜSSEN** im Eichtechnischen Log eichtechnisch relevante Ereignisse gespeichert werden, so dass nachträglich erkennbar ist, ob und welche Messwerte verfälscht worden sind.

Alle in der folgenden Tabelle identifizierten Ereignisse sind im Eichtechnischen Log zu protokollieren. Jeder Log-Eintrag **MUSS** dabei den Anforderungen aus Kapitel 5.2 genügen.

Ereignis / Parameter	*Eintrag*
Zuständige Eichbehörde	Die zuständige Eichbehörde bzw. Prüfstellenbezeichnung sowie das Eichjahr und alle diesbezüglichen Änderungen **MÜSSEN** im Eichtechnischem Log protokolliert werden.
Inbetriebnahme	Die Inbetriebnahme des SMGW **MUSS** im Eichtechnischem Log protokolliert werden.
Neuer Zähler	Der Anschluss und die Registrierung eines jeden neuen Zählers **MUSS** im Eichtechnischem Log protokolliert werden.
Entfernung eines Zählers	Die Loslösung eines Zählers vom SMGW **MUSS** im Eichtechnischem Log protokolliert werden.
Änderung von Konfigurationsprofilen	Jede Änderung (einschließlich Parametrierung) an Auswertungsprofilen gemäß Kapitel 4.4, sowie das Einbringen und Löschen von Auswertungsprofilen **MUSS** im Eichtechnischem Log protokolliert werden.
Softwareupdate	Jedes Update des eichtechnisch relevanten Softwareanteils **MUSS** im Eichtechnischen Log protokolliert werden.
Firmwareupdate	Jedes Firmwareupdate **MUSS** im Eichtechnischen Log protokolliert werden.
Fehlermeldung eines Zählers	Alle Fehlermeldungen der angeschlossenen Zähler **MÜSSEN** im Eichtechnischen Log protokolliert werden.

Tabelle 43: Obligatorische Einträge im Eichtechnischem Log

5.3.2 Obligatorische Einträge im Letztverbraucher-Log

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

Alle in der folgenden Tabelle identifizierten Informationen und Ereignisse sind im Letztverbraucher-Log zu protokollieren. Jeder Log-Eintrag **MUSS** dabei den Anforderungen aus Kapitel 5.2 genügen und mindestens für 15 Monate vorgehalten werden.

Ereignis / Information	*Beschreibung*
Kennung des Letztverbrauchers	Die eindeutige Kennung des Letztverbrauchers **MUSS** im Letztverbraucher-Log gespeichert sein.
Kennzeichnung des SMGW	Die eindeutige Bezeichnung des SMGW (Software, Firmware und Hardware) **MUSS** im Letztverbraucher-Log angezeigt werden.
Kennzeichnung der dem Kunden zugeordneten Zähler	Die eindeutige Bezeichnung der am SMGW angeschlossenen und dem Letztverbraucher zugeordneten Zähler **MUSS** im Letztverbraucher-Log angezeigt werden.
Hinzufügen oder entfernen von Zählern	Werden neue Zähler dem Letztverbraucher zugeordnet oder wurden Zähler entfernt oder ausgetauscht, so **MUSS** dies im Letztverbraucher-

Ereignis / Information	*Beschreibung*
	Log protokolliert werden.
Versenden von Daten	Jeder Datenverkehr vom SMGW an externe Marktteilnehmer und/oder den Gateway Administrator **MUSS** im Letztverbraucher-Log protokolliert werden. Ebenso **MUSS** jeder Aufbau einer Proxy-Verbindung protokolliert werden.
Aktuelle Auswertungsprofile	Alle aktiven sowie die unmittelbar vorhergehenden Auswertungsprofile sowie die zugehörige Parametrierung gemäß Kapitel 4.4 **MÜSSEN** im Letztverbraucher-Log protokolliert werden.
Änderung von Auswertungsprofilen	Jede Änderung (einschließlich Parametrierung) der Auswertungsprofile gemäß Kapitel 4.4 **MUSS** im Letztverbraucher-Log protokolliert werden.
Kennung des Lieferanten bzw. Rechnungstellers	Die Lieferanten bzw. Rechnungssteller der letzten 15 Monate **MÜSSEN** im Letztverbraucher-Log gespeichert werden.
Abrechnungsrelevante Daten	Alle Abrechnungsrelevanten Daten von mindestens 15 Monaten **MÜSSEN** im Letztverbraucher-Log gespeichert sein.
Status des Messsystems	Alle abrechnungsrelevanten Status- und Fehlermeldungen des SMGWs sowie der angeschlossenen und dem Letztverbraucher zugeordneten Zähler **MÜSSEN** im Letztverbraucher-Log protokolliert werden. Für den Letztverbraucher **MUSS** erkennbar sein, ob und welche Messwerte auf Grund von Fehlern ungültig sind und nicht zur Messwertbetrachtung herangezogen werden können.
Zuordnung zum Zählpunkt	Die aktuelle Zuordnung zu einem oder mehreren Zählpunkten sowie jedes Ändern, Hinzufügen oder Löschen von Zählpunkten.
Änderung der Zugangsdaten	Sind Zugangsdaten für das Letztverbraucher-Log geändert worden, so **MUSS** dies im Letztverbraucher-Log protokolliert werden.

2570 *Tabelle 44: Obligatorische Einträge im Letztverbraucher-Log*

6 Nicht-Funktionale Anforderungen

6.1 Einleitung

Dieses Kapitel hat informativen Charakter.

Neben den funktionalen Anforderungen an ein Smart Metering System, die in Kapitel 2 beschrieben wurden, existiert eine Reihe von nicht-funktionalen Anforderungen, die in den folgenden Kapiteln dargestellt werden.

6.2 Versiegelung

Das SMGW **MUSS** sich gegen Angriffe schützen, die einen lokalen Zugriff auf das SMGW voraussetzen. Gemäß [GW_PP] gilt hierbei, dass das unterstellte Angriffspotential in diesem Szenario limitiert ist.

Als Grundsatz gilt, dass durch eine Versiegelung des SMGW derselbe Schutzlevel erreicht werden **MUSS**, wie dies bei klassischen Zählern durch die Versiegelung bzw. Verwendung einer Plombe erreicht wird. Dieser Level wird durch spezifische Aspekte des SMGW ergänzt und durch die Anforderungen in diesem Kapitel beschrieben.

Das SMGW **MUSS** durch Verwendung eines geeigneten Siegels[23] physische Manipulationen erkennbar machen. Es **DARF NICHT** möglich sein, das Gehäuse des SMGW zu öffnen ohne das Siegel erkennbar zu brechen.

Das Siegel **MUSS** auf dafür geeigneten Siegelflächen angebracht werden, so dass es im normalen Betrieb nicht durch Abnutzung gebrochen wird.

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.

Das Siegel auf dem Gehäuse des SMGW **MUSS** in der gesicherten Produktionsumgebung des Herstellers angebracht werden. Das Siegel darf durch den Hersteller selbst angebracht werden.

Das 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

[23] Hinweis: Je nach Bauart des Gehäuses muss ggf. mehr als ein Siegel verwendet werden.

der SMGW-Admin 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.

6.3 Einbau des Sicherheitsmoduls

Zur gegenseitigen Authentisierung zwischen Smart Meter Gateway und Sicherheitsmodul wird das PACE-Verfahren verwendet [BSI TR-03109-3].

Die dafür benötigte PIN MUSS im SMGW geeignet geschützt werden . Der Hersteller des Gateways MUSS diesen Mechanismus von einer CC-Prüfstelle sicherheitstechnisch begutachten lassen und dies dem BSI in Form einer Herstellererklärung nachweisen.

Für das sicherheitstechnische Gutachten muss die Prüfstelle analog zu der [CEMV3.1] 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

7 Literatur- und Referenzverzeichnis

[BSI TR-03109-2] Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-03109-2, Smart Meter Gateway – Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls

[BSI TR-03109-3] Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-03109-3, Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen

[BSI TR-03109-4] Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-03109-4, Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways

[CCPart2V3.1] Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012, Part 2: Security functional components

[CEMV3.1] Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012, Evaluation methodology

[DIN 43863-5:2012-04] "Herstellerübergreifende Identifikationsnummer für Messeinrichtungen", DIN 43863-5:2012-04, DIN, 2012.

[DRAFT-IETF-AFT-SOCKS-SSL-00] „Secure Sockets Layer for SOCKS Version 5“, March 1997

[EER] Energieeffizienzrichtlinie „Richtlinie 2012/27/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur Energieeffizienz, zur Änderung der Richtlinien 2009/125/EG und 2010/30/EU und zur Aufhebung der Richtlinien 2004/8/EG und 2006/32/EG Text von Bedeutung für den EWR“, 25/10/2012

[EIA RS-485] EIA Standard RS-485, Electrical Characteristics of Generators and Receivers for Use in Balanced Multipoint Systems, ANSI/TIA/EIA-485-A-98, 1983/R2003.

[EN 13757-1] Kommunikationssysteme für Zähler und deren Fernablesung - Teil 1: Datenaustausch, März 2003, DIN EN 13757-1:2003-03

[EN 13757-3] Kommunikationssysteme für Zähler und deren Fernablesung - Teil 3: Spezieller Application Layer, Februar 2005, DIN EN 13757-3:2005-02

[EN 13757-4] Kommunikationssysteme für Zähler und deren Fernablesung - Teil 4: Zählerauslesung über Funk (Fernablesung von Zählern im SRD-Band von 868 MHz bis 870 MHz), Oktober 2005, DIN EN 13757-4:2005-10

[GW_PP] Protection Profile for the Gateway of a Smart Metering System, BSI-CC-PP-0073

[IEC 62056-6-1] Electricity metering – Data exchange for meter reading, tariff and load control – Part 6-1: COSEM Object Identification System (OBIS), 2011-10-10

[IEC 62056-46] Electricity metering – Data exchange for meter reading, tariff and load control – Part 46: Data link layer using HDLC protocol, 2002-02-18

[IEC 62056-5-3-8] Electricity metering – Data exchange for meter reading, tariff and load control – Part 5-3-8: Smart Message Language SML, 2012

[IEC 62056-6-2] Electricity metering – Data exchange for meter reading, tariff and load control – Part 6-2: Interface classes, FDIS IEC, Melbourne meeting, October 2011

[IEEE 802.3i] IEEE Std 802.3i-1990 (Clauses 13 and 14), 10 Mb/s UTP MAU, 10 BASE-T

[IEC/ISO 13239:2002] Information technology — Telecommunications and information exchange between systems — High-level data link control (HDLC) procedures, 2002

[M441-TR] Technical Report – Functional Reference Architecture for Communications in Smart Metering Systems, Final Draft CEN/CLC/ETSI/FprTR 50572:2011, SM-CG under Mandate M/441

[Derzeit PTB_A50.7ff] Anforderungen an elektronische und softwaregesteuerte Messgeräte und Zusatzeinrichtungen für Elektrizität, Gas, Wasser und Wärme, PTB, April 2002

[RFC1928] „SOCKS Protocol Version 5“, March 1996

[RFC2119] “Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, RFC 2119, March 1997

[RFC2616] “Hypertext Transfer Protocol – HTTP/1.1”, R. Fielding, et al., RFC 2616, June 1999

[RFC2617] “HTTP Authentication: Basic and Digest Access Authentication”, Franks, et al., RFC 2617, June 1999

[RFC5905] “Network Time Protocol Version 4: Protocol and Algorithms Specification”, D. Mills, et al., RFC 5905, June 2010

[SM_PP] Protection Profile for the Security Module of a Smart Metering System, BSI-CC-PP-0077

[VDE AR-N 4400:2011-09] Messwesen Strom (Metering Code), VDE-AR-N-4400, VDE, September 2011

8 Glossar und Abkürzungsverzeichnis

Dieser Anhang hat informativen Charakter.

Als Glossar und Abkürzungsverzeichnis dienen Kapitel 7.2 des Schutzprofils [GW_PP] sowie Anhang B von [M441-TR]. Diese Dokumente sind in englischer Sprache verfasst. Alle dort aufgeführten Begriffe gelten in der dort beschriebenen Bedeutung auch für diese Technische Richtlinie.

Folgende Begriffe werden in diesem Dokument zusätzlich in der unten definierten Bedeutung benutzt:

Abgeleitete Register	Container zur Aufnahme eines Datensatzes. Im Kontext der traditionell benutzten Formulierung entsprechen diese Container unter anderen den „Tarifregistern“ in einem Zähler. Abgeleitete Register beinhalten die neuen Messgrößen.
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 originäre Messwerte beinhalten.
Abrechnungsrelevanter Messwert	Ein mit einem geeichten und zertifizierten SMGW empfangener bzw. berechneter, gültiger und zeitgestempelter Zahlenwert einer Messgröße zuzüglich seiner Einheit.
Abrechnungstechnischer Kalendertag	Kalendertag, der für Abrechnungszwecke bei Strom um 0:00h und bei Gas um 6:00h beginnt.
Abrechnungszeitraum	Zeitraum, für den eine Abrechnung erstellt wird.
Auswertungsprofil	Ein Auswertungsprofil parametrisiert ein Regelwerk, für einen konkreten Anwendungsfall.
Bilanzierung	Siehe Bilanzkreisabrechnung.
Bilanzkreis	Ein Bilanzkreis ist ein virtuelles Gebilde, das sich aus einer beliebigen Anzahl von Einspeise- und Entnahmestellen zusammensetzt und zum Zweck des Ausgleichs zwischen Einspeisung und Entnahme gegenüber dem jeweiligen Übertragungsnetzbetreiber eingerichtet wird.
Bilanzkreisabrechnung	Gegenüberstellung von Energielieferungen und -bezügen für einen Bilanzkreis.
Einspeisung	Von einer Erzeugungs- oder Speicheranlage in ein Energienetz eingespeiste Energiemenge.

Energiemenge	Menge an Elektrizität oder Gas, soweit sie zur leitungsgebundenen Energieversorgung und Energieeinspeisung verwendet werden.[24]
Erzeugungsanlage	Anlage zur Erzeugung von Strom, 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 Letztverbraucher den Zähler eindeutig identifizieren kann.
Gültigkeitszeitraum	Der Zeitraum für den ein Regelwerk mit gleichbleibenden Parametern im SMGW arbeiten muss. Der Zeitraum kann im Fall einer Tarifabbildung an die Vertragslaufzeiten des Tarifs geknüpft sein.
HAN-Kommunikationsprofil	HAN-Kommunikationsprofile legen die Parameter für die Kommunikation des SMGW zu Letztverbrauchern oder Service-Technikern fest.
Kommunikationsprofil	Ein Kommunikationsprofil legt die Parameter für die Kommunikation zu einem autorisierten externen Marktteilnehmer im WAN oder dem SMGW-Admin fest.
Konfigurationsprofile	Oberbegriff für Auswertungsprofile, Kommunikationsprofile und Zählerprofile.
Lastgang	Gesamtheit periodisch erfasster Energiemengen über einen Zeitraum. Siehe auch Registrierende Lastgangmessung.
Laststufe	Einteilung einer Energiemenge, die in einem bestimmten Leistungsbereich verbraucht oder eingespeist worden ist. Laststufen sind spezielle Tarifstufen.
Letztverbraucherkennung	Der im SMGW eindeutige Bezeichner für einen Letztverbraucher.
Lieferant	Energielieferant, der seine Energie dem Letztverbraucher zur Verfügung und in Rechnung stellt.
Messgröße	Physikalische Größe, die gemessen wird.
Messsystem	Ein Messsystem ist eine in ein Kommunikationsnetz eingebundene Messeinrichtung zur Erfassung der Energiemenge, die den tatsächlichen Energieverbrauch bzw. Energieeinspeisung und den tatsächlichen Nutzungszeitraum widerspiegelt.
Messwert	Ein mit einem Messsystem gemessener und erfasster Zahlenwert einer Messgröße zuzüglich seiner Einheit.

[24] Bei Gas bezeichnet der Begriff Energiemenge das Gasvolumen.

Messwertliste	Eine Messwertliste enthält alle Messwerte eines Zählers, die für Messwertverarbeitungen in einem Regelwerk verwendet werden. Zusätzlich zum Messwert wird der Zeitstempel und die Statusinformation des Messwerts hinterlegt sowie der Grund für die Messwertverarbeitung. In der technischen Umsetzung kann die Messwerteliste über eine abgeleitete Werteliste modelliert werden.
Messwertsatz	Eine Menge von Messwerten.
Momentanleistung	Die von einem Zähler aktuell gemessene Leistung.[25]
Netzbetreiber	Betreiber von Energieversorgungsnetzen.
Netzzustandsdaten	Netzzustandsdaten sind nicht abrechnungsrelevante Messwerte, die für Betriebsführungszwecke benötigt werden (z.B. Spannung, Phasenwinkel, Frequenz) und die nicht für Tarifierung oder Bilanzierung verwendet werden.
Neue Messgröße	Vom SMGW aus physikalischen Messgrößen berechnete Messgröße. Messwerte neuer Messgrößen werden in abgeleiteten Registern abgelegt.
OBIS	Object Identification System. OBIS-Kennzahlen werden zur eindeutigen Identifikation von Messwerten und auch anderer abstrakter Daten verwendet.
Originärer Messwert	Ein mit einem Messgerät gemessener Zahlenwert einer Messgröße 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 Messwerten die mit zu sendende Geräte-ID des jeweiligen Zählers durch ein Pseudonym ersetzt, um die Identifizierung des Zählers und damit des Letztverbrauchers zu erschweren. Das verwendete Pseudonym wird jeweils vom SMGW-Admin vorgegeben.
Rechnungssteller	Derjenige, der auf Basis der abrechnungsrelevanten Messwerte Rechnungen an einen anderen Marktteilnehmer stellt.

[25] Die Momentanleistung darf nur dann zur Tarifierung herangezogen werden, wenn dies mit den eichtechnischen Vorgaben vereinbar ist.

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 Auswertungsprofil parametriert.
Registrierende Lastgangmessung	Erfassung der Energiemenge pro Registrierperiode. Die Gesamtheit der Energiemengen über einen Zeitraum stellt einen Lastgang dar.
Registrierperiode	Eine Registrierperiode ist der Zeitraum zur Ermittlung eines Energiemesswertes für einen Lastgang oder Zählerstandsgang.
Statusinformation	Zusätzliche Information zu einem Messwert.
Tarif	Siehe Tarifierung.
Tarifierung	Die Tarifierung ist ein Aufteilen der gemessenen elektrischen Energie bzw. Volumenmengen gemäß den hinterlegten Auswertungsprofilen in verschiedene Tarifstufen.
Tarifstufe	Eine Tarifstufe bezieht sich auf den Anteil einer Energiemenge, die mit einem eigenen Preis abgerechnet werden soll. Tarifstufen werden den abgeleiteten Register zugeordnet.
Tarifumschaltanweisung (Steuersignal)	Ein vom SMGW-Admin oder von einem autorisierten CLS übermittelte Anweisung für die Steuerung von Tarifumschaltungen im SMGW.
Tarifumschaltliste	Liste von Tarifumschaltzeitpunkten. Die Umschaltzeitpunkte können periodisch wiederkehrend sein. Der Liste ist auch ein Gültigkeitszeitraum zugeordnet sowie die OBIS-Kennzahl des entsprechenden abgeleiteten Registers (Tarifstufe).
Tarifumschaltzeitpunkt	Zeitpunkt zu dem in eine bestimmte Tarifstufe geschaltet werden soll. Diese werden in Auswertungsprofilen parametriert.
Tarifwechselliste	Liste von Tarifwechselzeitpunkten.
Tarifwechselzeitpunkt	Zeitpunkt zu dem in eine bestimmte Tarifstufe geschaltet worden ist. Hier sind die tatsächlichen aufgetretenen Ist-Zeitpunkte gemeint.
Verbrauch	Von einem Letztverbraucher verbrauchte Energiemenge.
Verbrauchsstufe	Tarifstufe, die bis zu einem bestimmten Verbrauch in Abrechnungszeitraum gilt.
Zähler	Ein Zähler ist ein Messgerät, das allein oder in Verbindung mit anderen Messeinrichtungen für die Ermittlung eines oder mehrerer Messwerte eingesetzt wird.

Zählerprofil	Ein Zählerprofil beschreibt die Konfiguration für das SMGW, die notwendig ist, um mit einem Zähler zu kommunizieren und die aktuellen Messwerte zu erfassen.
Zählerstand	Der Zählerstand ist ein Messwert eines Zählers. Gemessen wird die Energiemenge die bis zum jeweiligen Ablesezeitpunkt verbracht oder eingespeist wurde.
Zählerstandsgang	Gesamtheit periodisch erfasster Zählerstände über einen Zeitraum. Die Periodizität ist über die Registrierperiode gegeben.
Zählpunkt	Netzpunkt, an dem die Energiemenge gemessen wird.

2693

2694 Folgende Abkürzungen werden in diesem Dokument benutzt:

Abkürzung	***Beschreibung***
CLS	Controllable Local System
CMS	Cryptographic Message Syntax
EMT	Externer Marktteilnehmer
SMGW-Admin	Smart Meter Gateway Administrator
HAN	Home Area Network
KMU	Klein- oder mittelständisches Unternehmen
KWK	Kraft-/Wärmekopplung
LMN	Local Metrological Network
MAC	Message Authentication Code
MDL	Messdienstleister
MSB	Messstellenbetreiber
PKCS	Public Key Cryptography Standards
RLM	Registrierte Leistungsmessung
SMGW	Smart Meter Gateway
TLS	Transport Layer Security
TR	Technische Richtlinie
URI	Uniform Ressource Identifier
VNB	Verteilnetzbetreiber
WAN	Wide Area Network

9 Anhang A: Datenstruktur Wake-Up Paket

Dieser Anhang hat normativen Charakter.

Das Wake-Up Paket **MUSS** eine Geräteidentifizierung des adressierten SMGW und einen Zeitstempel enthalten. Diese Felder **MÜSSEN** mit dem privaten Schlüssel des SMGW Administrators für die Inhaltsdatensicherung signiert werden. Die Informationen im Wake-Up Paket sind nicht vertraulich und werden daher nicht verschlüsselt.

Das Wake-Up Paket **MUSS** folgenden Aufbau haben:

<table>
<tr><th>Feld</th><th>#Bytes</th><th>Beschreibung</th></tr>
<tr><td>Header</td><td>2</td><td>Header = „WU“ (ASCII “57h 55h” = “0101.0111b 0101.0101b”)</td></tr>
<tr><td>VersionId</td><td>1</td><td>Wake-Up Paket Version = 01h</td></tr>
<tr><td>RecipientId</td><td>9</td><td>Ein-eindeutige Geräte-Identifikation des SMGW.

Kodierung gemäß [DIN 43863-5:2012-04]

Byte[1]: Sparte (01h..0Fh): 0Eh=Kommunikation

Byte[2-4]: Herstellerkennzeichnung (3 ASCII Großbuchstaben) gemäß FLAG Registrierung.
Zum Beispiel: „BSI“ → 42 53 49h
Die Kodierung erfolgt „MSB first“.

Byte[5]: Fabrikationsblock (00h..FEh)

Byte[6-9]: Fabrikationsnummer rechtsbündig mit führenden Nullen (8 Dezimalstellen 0000 0000 - 9999 9999)
Die Kodierung erfolgt als 32 Bit Unsigned Integer und „MSB first“.

Zum Beispiel:

<table><tr><th colspan="9">RecipientId (9 Bytes)</th></tr><tr><td>K.</td><td colspan="3">„BSI“</td><td>„1“</td><td colspan="4">„0123 4567“</td></tr><tr><td>0E</td><td>42</td><td>53</td><td>49</td><td>01</td><td>00</td><td>12</td><td>D6</td><td>87</td></tr></table></td></tr>
<tr><td>Timestamp</td><td>8</td><td>UTC UnixTime als 64 Bit Signed Integer (Anzahl Sekunden seit dem 1. Januar 1970 00:00:00 UTC).

Zum Beispiel:
„13. Juli 2012 11:01:20 UTC“ →</td></tr>
</table>

Feld	*#Bytes*	*Beschreibung*
		„1.342.177.280d“ = „00 00 00 00 50 00 00 00h“ Die Kodierung erfolgt „LSB first“.
Padding / Reserved	12	Mit „0Bh“ gefüllter Anhang, damit der Datensatz 32 (2*16) Bytes lang wird. Gegebenenfalls für zukünftige Erweiterungen.
SignatureFormat	1	SignatureFormatTag: PlainFormat = 01h
SignatureAlgorithmOIDLength	1	Länge des folgenden SignatureAlgorithmObjectIdentifiers.
SignatureAlgorithmOID	0..14	OID des verwendeten Signaturalgorithmus gemäß [BSI TR-03109-3]. Zum Beispiel: ecdsa-plain-SHA256 ::= { itu-t(0) identified-organization(4) etsi(0) reserved(127) etsi-identified-organization(0) bsi-de(7) algorithms(1) id-ecc(1) signatures(4) ecdsa-plain-signatures(1) 3 }
SignaturePartR	*L*	Octet string R = I2OS(*r*; *L*) und $L = \log_{256}(r)$
SignaturePartS	*L*	Octet string S = I2OS(*s*; *L*) und $L = \log_{256}(s)$

Tabelle 45: Aufbau der Felder im Wake-Up Paket

Das Feld ***Header*** dient zur Kennzeichnung des Wake-Up Pakets und ermöglicht eine erste einfache (hardwarenahe) Überprüfung bzw. Klassifizierung der empfangen Pakete.

Das Feld ***VersionId*** bezeichnet die verwendete Version der Wake-Up Paket Definition. Bei eventuellen zukünftigen Erweiterungen werden neue Versionsnummern vergeben.

Das Feld ***RecipientId*** dient zur eindeutigen Identifizierung des SMGW. Die Vergabe und Kodierung der RecipientId **MUSS** gemäß [VDE AR-N 4400:2011-09] Kapitel 4.2 nach [DIN 43863-5:2012-04] "Herstellerübergreifende Identifikationsnummer für Messeinrichtungen" erfolgen. Nur das adressierte SMGW darf das Wake-Up Paket verarbeiten. Hiermit soll verhindert werden, dass das Wake-Up Paket von einem Angreifer missbraucht wird, um eine Vielzahl von SMGW in der Verantwortung eines SMGW Administrators zu einem gleichzeitigen TLS Call-Back zu verleiten (DoS-Attacke).

Das Feld ***Timestamp*** enthält die aktuelle Zeit (in UTC) zum Zeitpunkt der Erstellung des Wake-Up Pakets. Geringfügige Unterschiede zwischen den jeweiligen Uhrzeiten auf den Servern und den

SMGW sind üblich. Der Timestamp **MUSS** daher in einem festgelegten Zeitfenster relativ zur Uhrzeit des SMGW liegen.

Der Timestamp dient dazu, dass ein einzelnes Wake-Up Paket nicht mehrfach für den Aufbau von TLS-Kanälen wiederverwendet werden kann (Replay-Attacke).

Dem Feld Timestamp folgen 12 ***Padding*** Bytes, um den Datensatz auf 32 (2*16) Bytes aufzufüllen. Das letzte Byte enthält die Anzahl der vorher kodierten Paddingbytes.

Anschließend wird vom SMGW Administrator ein Hash gemäß [BSI TR-03109-3] über diesen n*16 Bytes Datensatz generiert. Der Hash wird mit ECDSA und einer elliptischen Kurve[26] gemäß [BSI TR-03109-3] signiert.

Das Feld ***SignatureFormat*** dient zur Kennzeichnung welches Signaturformat im Wake-Up Paket verwendet wurde. Bisher ist nur das „PlainFormat(1)“ vorgesehen.

Das Feld ***SignatureAlgorithmOIDLength*** enthält die kodierte Bytelänge des darauf folgenden SignatureAlgorithmObjectIdentifiers.

Das Feld ***SignatureAlgorithmOID*** enthält die OID des verwendeten Signaturalgorithmus gemäß [BSI TR-03109-3].

Die erzeugte ***ECDSA-Signatur (r, s)*** wird im "Plain Format" kodiert und an das Wake-Up Paket angehängt.

Das vollständige Wake-Up Paket sieht nun folgendermaßen aus:

[26] Die elliptische Kurve und damit die Größe der ECDSA-Signatur wird vorgegeben durch den im SMGW Administrator Zertifikat vorhandenen Signaturschlüssel.

Header (2 Bytes)		***Vers. (1 B)***	***RecipientId (9 Bytes)***								***Timestamp (8 Bytes)***			
‚W'	‚U'	01h	0Eh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh
Timestamp (continued)			***Padding / Reserved (11 Bytes + 1 Byte Padding-Length)***											
xxh	xxh	xxh	xxh	0Bh	0Bh	0Bh	0Bh	0Bh	0Bh	0Bh	0Bh	0Bh	0Bh	0Bh	0Bh
Sig. Frm	***OID Len***	***SignatureAlgorithmOID (OID-Length Bytes)***												
01h	0Ah	04h	00h	7Fh	00h	07h	01h	01h	04h	01h	*xx*h				
ECDSA-Signature (r) (L Bytes)														
xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh
xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh
xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh
ECDSA-Signature (s) (L Bytes)														
xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh
xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh
xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh

Tabelle 46: Struktur Wake-Up Paket

Die in Tabelle 46 abgebildete Struktur wird als Wake-Up Paket an das SMGW versendet.

10 Anhang B: Zertifikate im LMN

Dieser Anhang hat normativen Charakter.

Folgende Anforderungen werden an das Zertifikatsprofil im LMN gestellt:

- Kleine Zertifikatsgröße (zur Minimierung des Overheads im TLS-Handshake),
- Eindeutige Abbildung von SMGW- bzw. Zähler Identifikationsnummer (gemäß [DIN 43863-5:2012-04]) im Zertifikat,
- Angepasste Zertifikatsvalidierung für Embedded Systeme (d.h. ohne Datum+Uhrzeit oder direkten WAN-Zugriff)

Daraus ergeben sich die folgenden Anforderungen an Zertifikatsfelder und Wertebereiche, die unterstützt werden **MÜSSEN**:

Zertifikatsfeld		Wert
Version		V3
SerialNumber		Zufällig gewählte, eindeutige Nummer bestimmt vom SMGW (nicht länger als 8 Octets).
Signature		Gleicher Wert wie im Feld signatureAlgorithm.
Issuer	-	Leer
Validity	ValidFrom ValidTo	Die Nutzungszeit des Zertifikats ist 7 Jahre. Siehe [BSI TR-03109-3] Abschnitt 3.2.
Subject	-	Leer
SubjectPublicKeyInfo		Siehe [BSI TR-03109-3] Abschnitt A.1.2.
Extensions		
SubjectAltName	Othername=<BSI-OID>||<SMGW/Meter-ID>	Kodierung gemäß Definition der RecipientId in Kapitel 3.2.5.2.

Anmerkung: Auf die Verwendung der Extensions KeyUsage, PrivateKeyUsagePeriod, CertificatePolicies, IssuerAltName, BasicConstraints, ExtendedKeyUsage und CRLDistributionPoints soll verzichtet werden, da die Bedeutung und die Überprüfung dieser Extensions im LMN in der Regel nicht möglich bzw. nicht sinnvoll ist. Auch soll so die Zertifikatsgröße auf einen Minimum beschränkt werden, um den Overhead beim TLS-Handshake zu minimieren.

Es **MÜSSEN** die folgenden Prozesse in Verbindung mit Zertifikaten im LMN abgebildet werden:

- Aufbringen/Generierung initialer Zertifikate (Herstellen von „Direct-Trust“)

- auf dem SMGW
- auf dem Meter

- Zertifikatserneuerung/-austausch
  - auf dem SMGW
  - auf dem Meter

Die Rahmenbedingen für diese Prozesse sind durch [BSI TR-03109-3] Abschnitt 6.1.1 festgelegt. Für das Aufbringen der initialen Zertifikate **MUSS** das symmetrische Verfahren aus [BSI TR-03109-3] Kapitel 7 verwendet werden.

11 Anhang C: Zertifikate im HAN

Dieser Anhang hat normativen Charakter.

Folgende Anforderungen werden an das Zertifikatsprofil im HAN gestellt:

- Kleine Zertifikatsgröße (Minimierung vom Overhead im TLS-Handshake)
- Eindeutige Abbildung von der SMGW- und CLS-Identifikationsnummern im Zertifikat
- (Optional) Überprüfbarkeit des Zertifikats und Zertifikatsherausgebers (Zertifikat als Nachweis „Originalgerät von Hersteller XYZ“)
- Unterstützung von Zertifikatserneuerungsprozessen durch entsprechende Zertifikatsextensions (AuthorityKeyId:keyIdentifier und SubjectKeyIdentifier)
- Angepasste Zertifikatsvalidierung für Embedded Systeme (d.h. ohne Datum+Uhrzeit oder direktem WAN-Zugriff)
- (Optional) Sperrverwaltung (Blacklisting) von einzelnen Zertifikaten/Schlüssel (auf dem SMGW).

Zertifikatsprofil:

Zertifikatsfeld		***Wert***
Version		V3
SerialNumber		Zufällig gewählte, eindeutige Nummer bestimmt von der CA (nicht länger als 8 Octets).
Signature		Gleicher Wert wie im Feld signatureAlgorithm.
Issuer	<Subject DN vom Herausgeber CA>	Eindeutiger Name (Distinguished Name, DN) des Zertifikatsherausgebers. Identisch mit dem SubjectDN für „Self-Signed“ Zertifikate.
Validity	ValidFrom ValidTo	Die Nutzungszeit des Zertifikats ist 7 Jahre. Siehe [BSI TR-03109-3] Kapitel 5.
Subject	<Subject DN vom CLS>	Eindeutiger Name (Distinguished Name, DN) des CLS. Alle DN-Felder sind Optional. Ein leerer SubjectDN ist zulässig.
SubjectPublicKeyInfo		Siehe [BSI TR-03109-4] Abschnitt A.1.2.
Extensions		
SubjectAltName:	Othername=<BSI-OID>|<SMGW/CLS-ID>	Ein-eindeutige Geräte-Identifikation des SMGWs bzw. des HAN Gerätes
AuthorityKeyId:	keyIdentifier	SubjectKeyIdentifier des Zertifikatsherausgebers.
SubjectKeyIdentifier		SubjectKeyIdentifier des Zertifikatsinhabers.

Zertifikatsfeld		*Wert*
SignatureAlgorithm		Siehe [BSI TR-03109-4] Abschnitt A.1.1.
SignatureValue		Abhängig vom gewählten Signaturalgorithmus.

Anmerkung: Auf die Verwendung der Extensions KeyUsage, PrivateKeyUsagePeriod, CertificatePolicies, IssuerAltName, BasicConstraints, ExtendedKeyUsage und CRLDistributionPoints soll verzichtet werden, da die Bedeutung und die Überprüfung dieser Extensions im HAN in der Regel nicht möglich bzw. sinnvoll ist. Auch soll so die Zertifikatsgröße auf einen Minimum beschränkt werden, um den Overhead beim TLS-Handshake zu minimieren. Für Hersteller und SMGW-Admin CAs werden keine speziellen Vorgaben gemacht.