Das SMGW kann weitere Parameter für Zählerprofile unterstützen. Zählerprofile werden über die „logical names" der Zähler in Auswertungsprofilen referenziert.

2. Auswertungsprofil einspielen

VORAUSSETZUNG
Vor der Aktivierung des Auswertungsprofils muss das SMGW folgende Punkte sicherstellen:

- Ein gültiger Tarifanwendungsfall muss vorhanden sein.
- Durch Geräte-ID referenzierte Zähler sind durch Zählerprofile konfiguriert.
- Die im Auswertungsprofil angegebenen OBIS-Kennzahlen für Messgrößen sind auch im jeweiligen Zählerprofil hinterlegt.
- Alle referenzierten Kommunikationsprofile sind im SMGW vorhanden.

Wird einer der Punkte nicht erfüllt, wird das Auswertungsprofil nicht aktiviert und ein entsprechender Eintrag ins System-Log des SMGW geschrieben.

Ein Auswertungsprofil parametrisiert ein Regelwerk für einen konkreten Anwendungsfall. Sie müssen folgende Parameter beinhalten:

Parameter	Datentyp/Wertebereich	Beschreibung
Bezeichner	Alphanummerisch	Im SMGW eindeutige Bezeichnung für das Auswertungsprofil.
Name	Text	Ein Name für das Auswertungsprofil.
Auswahl des Anwendungsfalles	Nummer	Dieser Parameter legt den Anwendungsfall (TAF) fest.
Parameter des (TAF)	Alphanummerisch	Alle für den jeweiligen Anwendungsfall notwendigen Parameter.
Optional die vom SMGW durchzuführenden Prüfungen der Messwerte		Abrechnungsrelevante Statusinformationen des Zählers.

Zugeordnete Kommunikationsprofile	1:n Bezeichner	Die Bezeichner referenzieren die Kommunikationsprofile, die für den Versand von verarbeiteten Messwerten an externe Marktteilnehmer verwendet werden.

Zählerprofile: Parameter

ⓘ Das SMGW kann weitere Parameter für Auswertungsprofile unterstützen.

Modellierung der Datenstrukturen des SMGW für Metering und Administration 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] realisieren.

3. Kommunikationsprofile für die WAN-Kommunikation einspielen

ⓘ Das Einspielen des Kommunikationsprofils für den EMT (INFO-REPORT) geschieht in Verbindung mit dem Auswertungsprofil.

⚠ VORAUSSETZUNG
Vor der Aktivierung des Kommunikationsprofils muss das SMGW folgende Punkte sicherstellen:

- Es muss mindestens ein WAN-Kommunikationsprofil mit der Rolle „GWA" 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 GWA müssen in den WAN-Kommunikationsprofilen ausschließlich die Kommunikationsszenarien MANAGEMENT und ADMIN-SERVICE zugeordnet werden.
- Das SMGW prüft vor der Deaktivierung eines Kommunikationsprofils, dass kein Auswertungsprofil auf das zu deaktivierende Kommunikationsprofil verweist.

ⓘ Wird einer der Punkte nicht erfüllt, wird das Kommunikationsprofil nicht aktiviert und ein entsprechender Eintrag ins System-Log des SMGW geschrieben.

Kommunikationsprofile müssen die folgenden Parameter beinhalten:

Parameter	Datentyp / Wertebereich	Beschreibung
Bezeichner	Alphanummerisch	Die im SMGW eindeutige Bezeichnung des Kommunikationsprofils.
Name	Text	Ein verständlicher Name für das Kommunikationsprofil.
Kommunikationsszenario	MANAGEMENT, ADMIN-SERVICE, INFO-REPORT, NTP-HTTPS, NTP-TLS	Legt das Kommunikationsszenario fest.
Rolle des Kommunikationspartners	Einer aus: SMGW-Admin EMT	Legt die Rolle des Kommunikationspartners fest.
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 offen gehalten 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 offen gehalten werden soll. Ein Wert größer als 48 h darf vom SMGW nicht akzeptiert werden.
Zertifikat des externen Markteilnehmers für die TLS-	Zertifikat	Das Zertifikat des externen Marktteilnehmers für die TLS-Authentifizierung durch das SMGW.

Authentifizierung		
Zertifikat des externen Markteilnehmers für die Signierung der Inhaltsdaten	Zertifikat	Das Zertifikat des externen Marktteilnehmers für die 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.
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 zur 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 zur Entschlüsselung von Inhaltsdaten im SMGW verwendet werden muss.

Zählerprofile: Parameter

ⓘ Das SMGW kann weitere Parameter für WAN-Kommunikationsprofile unterstützen.

4.2 Zeitsynchronisierung

Wird das SMGW erstmalig in Betrieb genommen, muss zunächst eine Zeitsynchronisierung durchgeführt werden. Da aufgrund der fehlenden Zeit keine Gültigkeitsprüfung der Zertifikate möglich ist, entfällt diese in diesem besonderen Fall.

5 Erklärung der Sicherheitsfunktionen

5.1 Logbücher

Das SMGW protokolliert seine Aktionen und Reaktionen in drei unterschiedlichen Arten von Logs:

- System-Log
- Eich-Log
- Letztverbraucher-Log

Der Zugriff auf diese Logs erfolgt gemäß folgender Tabelle:

Log	Zugriff	Schnittstelle
System-Log	lesender Zugriff durch den GWA	WAN-Schnittstelle
System-Log	lesender Zugriff durch den Service-Techniker	HAN-Schnittstelle (IF_GW_SRV)
Eich-Log	lesender Zugriff durch den GWA	WAN-Schnittstelle
Letztverbraucher-Log	lesender Zugriff durch den Letztverbraucher	HAN-Schnittstelle (IF_GW_CON)

5.1.1 Das System-Log

Abfrage Systemlog:

HTTP GET auf /smgw/cosem/ldevs/<smgw-id>/objects/0000636201ff

Das System-Log informiert den GWA und den autorisierten Service-Techniker über den Systemstatus des SMGW. Daher protokolliert das SMGW in diesem Log jedes wichtige Ereignis (z. B. Fehlermeldungen, Ausfall der WAN-Verbindung, sicherheitsrelevante Ereignisse, Aktivitäten des GWA, etc.).

ⓘ Es werden keine datenschutzrelevanten Informationen im System-Log gespeichert.

ⓘ Beachten Sie, dass niemand die Ereignisse löschen oder bearbeiten kann, die im Letztverbraucher-Log aufgezeichnet werden.

Dieses Log kann nur von dem autorisierten GWA sowie dem autorisierten Service-Techniker vor Ort eingesehen werden. Die Informationen dienen aus-

schließlich dazu, den momentanen Status des SMGW zu erkennen und eventuelle Fehlerquellen oder Störungen zu identifizieren.

Das SMGW wertet auditierte Ereignisse aus, um potenzielle Sicherheitsverletzungen auszumachen. Dabei finden mehrere Regeln Anwendung.

Der GWA kann zusätzlich eine Anzahl von auditierbaren Ereignissen auswählen, die einen potenziellen Sicherheitsverstoß darstellen.

Bei Erkennen einer möglichen Sicherheitsverletzung erzeugt das SMGW einen Log-Eintrag im System-Log und informiert den GWA über das Kommunikationsszenario **ADMIN-Service**.

Ist das System-Log voll, beginnt das SMGW damit, die ältesten Ereignisse zu überschreiben.

5.1.2 Das Eich-Log

Abfrage Eichlog:

HTTP GET auf /smgw/cosem/ldevs/<smgw-id>/objects/0000636202ff

Im Eich-Log werden eichrechtlich relevante Ereignisse (z. B. erkannte Verfälschungen von Messungen, fehlgeschlagene Zeitsynchronisierungen) dauerhaft und nachvollziehbar gespeichert. Außerdem erfolgt die Registrierung von Änderungen an eichrechtlich relevanten Parametern (z. B. das Stellen der Geräteuhr). Jeder Eintrag in diesem Logbuch ist durch eine digitale Signatur des SMGW vor nachträglicher absichtlicher oder unbeabsichtigter Verfälschung geschützt.

ⓘ Beachten Sie, dass niemand die Ereignisse löschen oder bearbeiten kann, die im Letztverbraucher-Log aufgezeichnet werden.

Nur der GWA kann das Eich-Log lesen, aber keine gespeicherten Ereignisse löschen oder modifizieren.

Die Ereignisse werden z. B. im Eich-Log gespeichert:

Für den Fall, dass das Eich-Log voll sein sollte, stoppt das SMGW den Messbetrieb, erzeugt einen Log-Eintrag im System-Log und informiert den GWA.

Um sicherzustellen, dass die Ereignisse über die gesamte Lebenszeit des SMGW zur Verfügung stehen, sieht das Gateway genügend Speicherplatz vor.

Logdaten abrufen

Die Logdaten sind für den GWA wie folgt abrufbar:

Mögliche Parameter:

- **Ausgabe aller Einträge zwischen Start- und Endzeitpunkt**
  ?q.fromtime=<Startzeitpunkt>&q.totime=<Endzeitpunkt>

- **Ausgabe einer bestimmten Anzahl Einträge beginnend vom Startzeitpunkt**
  ?q.fromtime=<Startzeitpunkt>&q.count=<Anzahl Einträge>
- **Ausgabe einer bestimmten Anzahl Einträge beginnend vom angegebenen Index**
  ?q.fromidx=<Startindex>&q.count=<Anzahl Einträge>

ⓘ Werden keine Parameter angegeben, wird das gesamte Logbuch ausgegeben. Das ausgegebene Logfile entspricht in seinem Aufbau den Vorgaben aus der DKE.

Jeder ausgelesene Log-Eintrag beinhaltet folgende Informationen:

Merkmal	Bedeutung o/m/c22	o/m/c22
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
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.	m

	– 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.	
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
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

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

Log-Eintrag und Bedeutung

5.1.3 Letztverbraucher-Log

Das Letztverbraucher-Log hält für Letztverbraucher abrechungsrelevante Daten und Tarifinformationen bereit, so dass dieser die Möglichkeit erhält, nachzuvollziehen, welche Messwerte für die Abrechnung verwendet werden. Des Weiteren kann der Letztverbraucher dadurch erfahren, welche Daten an externe Marktteilnehmer versendet werden. Hierfür protokolliert das SMGW alle diesbezüglichen Ereignisse.

ⓘ Beachten Sie, dass niemand die Ereignisse löschen oder bearbeiten kann, die im Letztverbraucher-Log aufgezeichnet werden.

Ist das Letztverbraucher-Log voll, beginnt das SMGW damit, die ältesten Ereignisse zu überschreiben. Beim Überschreiben aller Einträge im Log informiert das SMGW den GWA einmal pro Zyklus und erzeugt einen entsprechenden Log-Eintrag im System-Log.

Der GWA wird informiert, da er die Größe des Letztverbraucher-Logs konfigurieren kann. Der GWA muss sicherstellen, dass genügend Speicherplatz zum Aufzeichnen von Ereignissen im Letztverbraucher-Log für mindestens 15 Monate zur Verfügung steht.

5.2 Teilnehmer-/Nutzer- und Zugriffsberechtigungen

5.2.1 Grundsätzliche Zugriffsbeschränkungen

Generell gilt, dass kein geheimes Schlüsselmaterial aus dem SMGW ausgelesen werden kann. Jeder Zugriff ist zweckgebunden und über Zugriffsrechte organisiert.

5.2.2 Berechtigungen für den Service-Techniker

Der Service-Techniker kann, abhängig von der Personalisierung, ausschließlich die folgenden Informationen im SMGW einsehen:

- Das System-Log des SMGW.
- Weitere Diagnose-Informationen.

5.2.3 Berechtigungen für den Letztverbraucher

Ein Letztverbraucher kann folgende, nur ihn betreffende Informationen einsehen:

- Die für ihn im SMGW konfigurierten Zähler.
- Auswertungsprofile.
- Kommunikationsprofile.
- Zählerstände und Messwertlisten.

- Eigene aktuelle und vergangene Verbrauchs- und/oder Einspeisewerte sowie
- das eigene Letztverbraucher-Log.

ⓘ Der Letztverbraucher kann keine Daten einsehen, die andere Letztverbraucher betreffen.

5.2.4 Berechtigungen für externe Marktteilnehmer (EMT)

Autorisierte externe Marktteilnehmer sind aus Sicht des SMGW alle Teilnehmer mit Ausnahme des SMGW 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.

5.2.5 Berechtigungen für den Gateway-Administrator (GWA)

Ein GWA konfiguriert und überwacht das SMGW.
Er hat folgende Zugriffsberechtigungen:

- Zugriff zum Zweck der Konfiguration des SMGW. Dies betrifft insbesondere:
  - die Konfiguration für Messwerterfassung, Messwertverarbeitung und Versand von Messwerten und anderen Informationen an EMT.
  - die Konfiguration der Zugriffsberechtigungen für EMT.
  - die Einspielung von Firmware-Updates nach Überprüfung der Authentizität und Funktion der Firmware.
  - die Konfiguration des Zertifikatsmaterials im SMGW.
- Lese-Zugriff zur Einsichtnahme in das Eichtechnische-Log und das System-Log. Er darf aber keine Änderungen an diesen Logs vornehmen.
- Ausführen eines Wake-Up.

Weitere Zugriffe auf das SMGW sind nicht gestattet.

5.3 Zugriffsberechtigungen konfigurieren

5.3.1 Für die Nutzerrollen erforderliche Parameter

Jeder Nutzer, der mit dem SMGW kommuniziert oder Daten vom SMGW erhält, wird vor jeder Aktion (z. B. dem Empfang vom Gateway gesendeten Daten) identifiziert und authentifiziert. Hierfür erhält das SMGW die folgenden Merkmale für jeden Nutzer:

- Die Nutzeridentität.
- Den Status der Identität (authentifiziert oder nicht).

- Das Verbindungsnetzwerk (WAN, HAN oder LMN).
- Die Rolle und
- das Datum der Aktivierung.

Innerhalb des Prozesses der Erstverbindung oder bei Änderung der Sicherheitsattribute eines Nutzers prüft das SMGW, ob die folgenden Regeln angewendet werden:

- Die Eigenschaft der Rolle entspricht nur einem der folgenden Werte:
  - autorisierter Verbraucher.
  - autorisierter GWA.
  - autorisierter Service-Techniker.
  - autorisierter Zähler.
  - autorisiertes CLS oder
  - autorisierter externer Marktteilnehmer.
- Ist der Nutzer ein autorisierter GWA, darf das Sicherheitsattribut des Verbindungsnetzwerks nur WAN sein.
- Ist der Nutzer ein autorisierter externer Marktteilnehmer, darf das Sicherheitsattribut des Verbindungsnetzwerks nur WAN sein.
- Ist der Nutzer ein autorisierter Letztverbraucher, darf das Sicherheitsattribut des Verbindungsnetzwerks nur HAN sein.
- Ist der Nutzer ein autorisierter Service-Techniker, darf das Sicherheitsattribut des Verbindungsnetzwerks nur HAN sein.
- Ist der Nutzer ein autorisiertes CLS, darf das Sicherheitsattribut des Verbindungsnetzwerks nur HAN sein.
- Ist der Nutzer ein autorisierter „Meter", darf das Sicherheitsattribut des Verbindungsnetzwerks nur LMN sein.

5.4 Kommunikationsprotokolle

Zur Sicherung der Kommunikationswege von und zum SMGW werden verschiedene Kommunikationsprotokolle angewendet.

5.4.1 Sicherung der Kommunikation mit Transport Layer Security (TLS)

Beim Aufbau eines TLS-Kanals werden folgende Funktionen des Sicherheitsmoduls verwendet:

- Die Generierung von Zufallszahlen für das TLS-Kommando **ClientHello**.
- Der Schlüsselaustausch des TLS „pre-master secrets" gemäß Elliptic Curve Diffie-Hellman sowie
- die Signaturerzeugung und -prüfung zur Authentifizierung.

Zur gegenseitigen Authentifizierung zwischen dem SMGW und Zählern im LMN werden selbst-signierte X.509-Zertifikate eingesetzt.

5.4.2 Proxy-Kommunikationsprofil

Für die transparente Datenkommunikation zwischen einem CLS und einem externen Marktteilnehmer ist die Konfiguration von Proxy-Kommunikationsprofilen erforderlich. In einem Proxy-Kommunikationsprofil wird ein CLS mit einem bestimmten externen Marktteilnehmer verknüpft, indem die Kommunikationsparameter der beiden Endpunkte spezifiziert werden. Es können mehrere Proxy-Kommunikationsprofile je CLS oder externem Marktteilnehmer definiert werden. Für ein bestimmtes Paar aus externem Marktteilnehmer und CLS kann aber jeweils nur ein Proxy-Kommunikationsprofil aktiv sein.

Die Proxy-Kommunikationsprofile legen die Parameter für den Aufbau eines transparenten Kommunikationskanals zwischen einem externen Marktteilnehmer und einem CLS fest. Proxy-Kommunikationsprofile können ausschließlich vom GWA eingespielt werden.

5.5 Identifizierung und Authentifizierung

Die Authentifikation des GWA und aller externen Marktteilnehmer an der WAN-Schnittstelle wird nur über Zertifikate durchgeführt, die der Smart-Metering-Public-Key-Infrastruktur entstammen. Zusätzlich wird jeder Befehl eines GWA über die Befehlsignatur verifiziert.

Letztverbraucher an der HAN-Schnittstelle können zwischen einer Authentifikation über Zertifikate oder über Nutzername und Passwort wählen. Diese Zertifikate werden auch zur Authentifizierung von Service Technikern und von CLS verwendet. Im Falle einer Letztverbraucher-Authentifikation über Nutzername und Passwort wird die erforderliche Information an das SMGW per HTTP-Digest-Access-Authentifikation übermittelt.

Für den Authenfizierungsmechanismus über Nutzername und Passwort muss der GWA die Schwelle für erfolglose Authenfizierungsversuche festlegen. Dabei

muss die Schwelle einer ganzen Zahl zwischen 3 und 10 erfolglosen Authenfizierungsversuchen entsprechen. Der voreingestellte Wert ist 5. Wenn die definierte Anzahl an erfolglosen Authentifizierungsversuchen erreicht ist, informiert das SMGW den GWA, erzeugt einen Eintrag im Letztverbraucher-Log (sofern die Nutzer-Identification (ID) bekannt ist), erzeugt einen Eintrag im System-Log und sperrt den Nutzer-Account für 5 Minuten.

Nach einer erfolgreichen Authentifizierung eines Letztverbrauchers wird der Zähler für erfolglose Authenfizierungsversuche für den Letztverbraucher auf null gesetzt. Wenn authentifizierte lokale Nutzer im HAN für mehr als 10 Minuten inaktiv sind, ist eine Re-Authentifizierung gemäß den oben beschriebenen Authentifizierungsregeln erforderlich. Anderenfalls wird die nächste Kommunikationsanfrage fehlschlagen.

5.6 Authentifizierung mittels Kennung und Passwort

Beim Aufbau einer TLS-Verbindung zwischen dem Letztverbraucher und dem SMGW wird im „TLS-Handshake" mit dem Zertifikat **GW_HAN_TLS_CRT** eine Server-Authentifizierung durchgeführt. Anschließend werden mit der Hypertext Transfer Protocoll (HTTP)-Digest-Access-Authentifizierung die Kennung und das Passwort des Letztverbrauchers abgefragt und an das SMGW übermittelt. Kennung und Passwort sind dabei eindeutig einem dem SMGW bekannten Letztverbraucher zugeordnet. Dies stellt sicher, dass nur Daten übermittelt werden, die dem authentifizierten Letztverbraucher zugeordnet sind.

5.7 Kryptografische Funktionen

Alle Verbindungen zum SMGW über WAN, HAN oder LMN sind kryptografisch gesichert.

5.7.1 Die Inhaltsdatensicherung

Da bestimmte Zähler-Daten vom SMGW über einen Dritten an externe Marktteilnehmer übertragen werden können, z. B. den GWA, ist der Dateninhalt immer verschlüsselt, „Message Authentication Code" (MAC)-gesichert und für die zugehörigen externen Marktteilnehmer gekennzeichnet.

Hierbei wird sichergestellt, dass dieses Schlüsselpaar sicher und gemäß BSI-TR-03109-3 generiert wird. Die zufällig erzeugten und nochmals verschlüsselten Schlüssel für die Key Encryption und die MAC-Sicherung der übertragenen Zähler-Daten sind im „Cryptographic Message Syntax" (CMS)-Container enthalten, der an den externen Marktteilnehmer gesendet wird.

Um die externen Marktteilnehmer in die Lage zu versetzen, den Ursprung der erhaltenen Meter-Daten zu überprüfen, kennzeichnet das Gateway die verschlüsselten und MAC-gesicherten Daten. Das SMGW verschlüsselt seine lokalen sicherheitsrelevanten Nutzerdaten während der Speicherung in einem persistenten Speicher.
Dieser Schlüssel wird ebenfalls mit dem Zufallszahlengenerator des Sicherheitsmoduls erzeugt.

Ephemeral Cryptographic Keys

Alle Ephemeral Cryptographic Keys, die für TLS- oder symmetrische Advanced Encryption Standard (AES)-Verschlüsselung verwendet werden, werden mit der Methode „Zeroization" gemäß zerstört. Hierfür überschreibt das SMGW den Random Access Memory (RAM)-Bereich, in dem diese Schlüssel gespeichert sind, mit Nullen, wenn diese nicht mehr benötigt werden. Dieser RAM-Bereich ist der einzige Ort, an dem Ephemeral Cryptographic Keys gespeichert werden.

5.7.2 HAN- und WAN-Zertifikate

HAN- und WAN-Zertifikate dienen der Identifizierung und Authentifizierung. Dabei werden zur Identifizierung und Authentifizierung von Service-Technikern, Letztverbrauchern und CLS-Komponenten gegenüber dem SMGW ausschließlich HAN-Zertifikate verwendet.

ⓘ Letztverbraucher können sich außerdem auch mittels Benutzername und Passwort identifizieren und authentifizieren.

Die Benutzeridentitäten (Letztverbraucher, Service-Techniker und CLS) und deren Zertifikate bzw. Kennung und Passwort müssen im SMGW registriert bzw. konfiguriert sein, damit sie vom SMGW als vertrauenswürdig akzeptiert werden. Dabei können einem Letztverbraucher auch mehrere Zertifikate oder Kennungen und Passwörter zugeordnet werden, beispielsweise für mehrere Anzeigeeinheiten oder CLS mit Datenzugriff.

TLS-Verbindung zwischen einem Teilnehmer im HAN und dem SMGW

Beim Aufbau einer TLS-Verbindung zwischen einem Teilnehmer im HAN und dem SMGW wird im TLS-Handshake mit den Zertifikaten **GW_HAN_TLS_CRT** und **CON_HAN_TLS_CRT** und deren 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. Dies stellt sicher, dass nur Daten übermittelt werden, die dem authentifizierten Letztverbraucher oder Service-Techniker zugeordnet sind.

TLS-Verbindung zwischen einem CLS und einem externen Marktteilnehmer

Beim Aufbau einer TLS-Verbindung zwischen einem CLS und dem SMGW wird ein (SOCKS)-TLS-Handshake mit den Zertifikaten **GW_HAN_TLS_CRT** und **CLS_HAN_TLS_CRT** und der zugehörigen Schlüssel eine Client-Server-Authentifizierung durchgeführt. Das Zertifikat **CLS_HAN_TLS_CRT** ist dabei eindeutig einem dem SMGW bekannten CLS zugeordnet. Das CLS teilt dem SMGW mit, zu welchem externen Marktteilnehmer eine Verbindung aufgenommen werden soll. Im SOCKS-Protokoll wird als Zieladresse ein eindeutiger Bezeichner für den externen Marktteilnehmer an das SMGW übermittelt. Das SMGW überprüft mittels der konfigurierten Proxy-Kommunikationsprofile die Zulässigkeit der Proxy-Verbindung und baut eine TLS-Verbindung zum externen Marktteilnehmer auf. Dabei wird eine Client-Server-Authentifizierung mit den Zertifikaten **GW_WAN_TLS_CRT** und **EMT_WAN_TLS_CRT** durchgeführt.

TLS-Verbindung zwischen einem externen Marktteilnehmer und einem CLS

Will ein externer Marktteilnehmer mit einem CLS kommunizieren, teilt er dem GWA die gewünschte Zieladresse des CLS mit.

5.7.3 Zertifikate zur Zeitsynchronisation

ⓘ Wenn das SMGW die Gültigkeit der internen Uhrzeit nicht sicherstellen kann, muss es eine Zeitsynchronisation durchführen. Für diese entfällt dann die Gültigkeitsprüfung der Zertifikate.

5.7.4 Pseudonymisierung von Daten

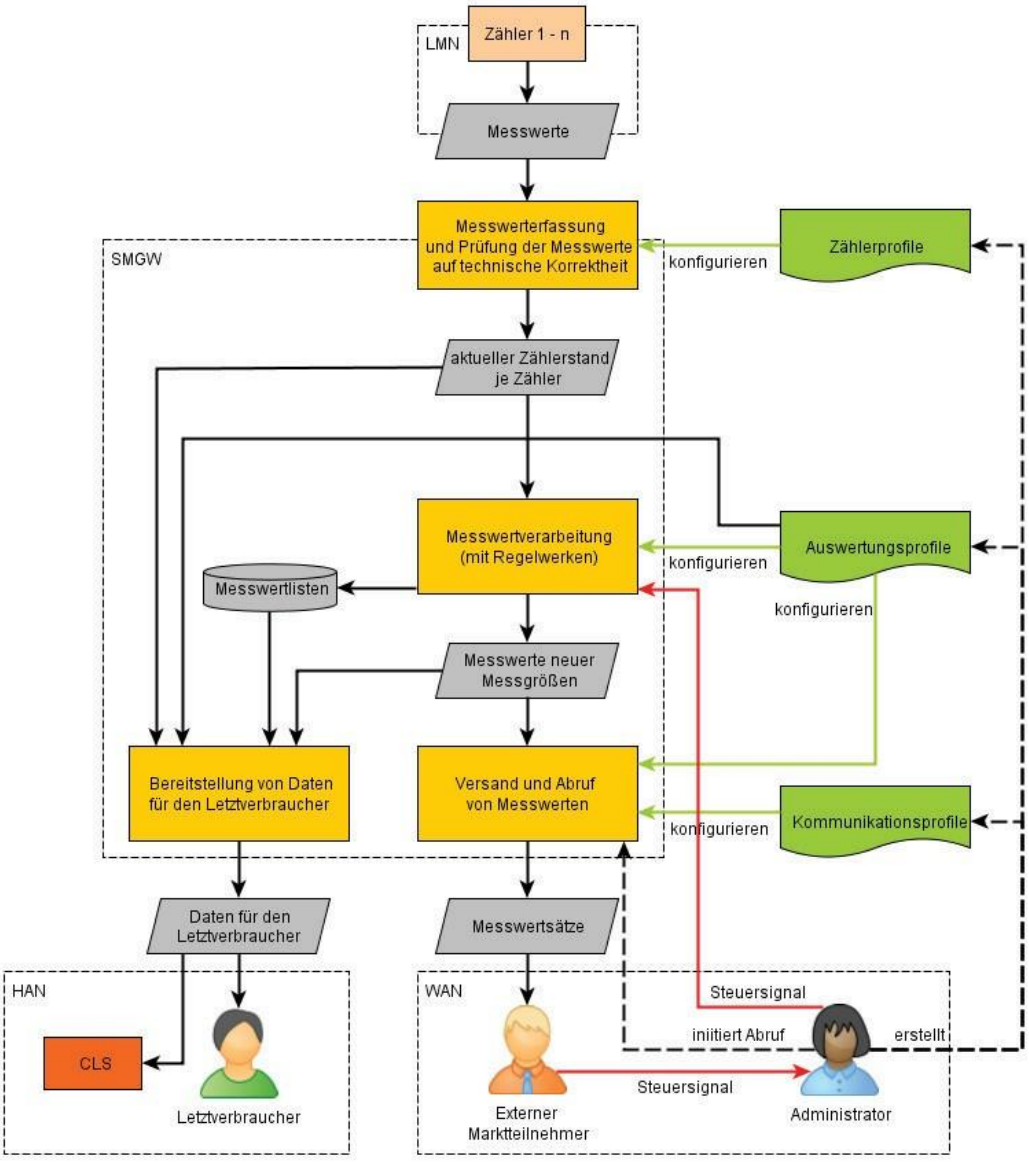
Die Pseudonymisierung von Netzzustandsdaten bei der Übertragung vom SMGW an einen externen Marktteilnehmer erfolgt durch folgende Schritte:

- Die Geräte-ID wird durch das SMGW aus den Messwerten entfernt und durch ein im Auswertungsprofil hinterlegtes Pseudonym ersetzt.
- Der Empfänger entschlüsselt die Daten.

Auf diese Weise wird verhindert, dass der Empfänger die Daten einem Letztverbraucher zuordnen kann.

6 Messwerte

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.



Zähler und Meßwerte

6.1 Messwerterfassung

Das SMGW erfasst Zählerstände von mehreren angeschlossenen Zählern. Die Parameter der Konfiguration werden durch die Zählerprofile eingegeben.

Voraussetzung:

- Gültiges Zählerprofil muss bereits eingespielt sein.
  Nach Einspielen des Zählerprofils ist der Zähler über seine Geräte-ID im SMGW eindeutig identifizierbar und adressierbar.
- Jedem Zähler muss ein Letztverbraucher zugeordnet sein, dessen Einspeisung er misst.

6.2 Messwertverarbeitung

Die Parameter der Konfiguration werden durch die Auswertungsprofile bzw. die TAF's eingegeben. Ein Gültigkeitszeitraum legt fest, ab welchem Zeitpunkt das Regelwerk für einen Anwendungsfall in Kraft treten soll und zu welchem Zeitpunkt es wieder deaktiviert wird.

Voraussetzung:

- Gültiges Auswertungsprofil mit beinhaltetem Tarifanwendungsfall

6.3 Messwertversand

Der Messwertversand wird über das Kommunikationsprofil definiert.

Voraussetzung:
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.
- Ggf. Statusinformation.

Das SMGW hinterlegt die oben genannten Informationen auch im Letztverbraucher-Log des jeweiligen Letztverbrauchers.

7 Funktionen und Bedienung

7.1 Messwerte für Tarifierung, Bilanzierung und Netzzustandsdaten-erhebung

Das SMGW kann die Zählerstände von mehreren angeschlossenen Zählern erfassen, wobei jeder Zähler über seine Geräte-ID eindeutig identifizierbar und adressierbar ist. Im Folgenden 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 erhebt das SMGW auch Messdaten, die von Netzbetreibern u. a. für die Bilanzierung von Energienetzen verwendet werden.

7.1.1 Anwendungsfälle

In diesem Kapitel werden die Anwendungsfälle für Tarifierung, Bilanzierung und Netzzustandsdatenerhebung beschrieben, die das SMGW erfüllen kann.

Der externe Marktteilnehmer erhält bei jedem Anwendungsfall die folgenden Informationen vom SMGW:

- die Messwertliste.
- die Tarifwechselliste, falls vorhanden.

Zähler und Messwertgrößen werden über die Geräte-IDs der Zähler und die OBIS-Kennzahlen der zu erfassenden Messgrößen ausgewählt. Das SMGW versieht die Daten vor der Inhaltsdatenverschlüsselung mit einer zusätzlichen Signatur. Zu einem festgelegten Zeitpunkt wird die Messwertliste dann an die berechtigten Marktteilnehmer versendet. Ein Gültigkeitszeitraum legt fest, ab welchem Zeitpunkt das Regelwerk für einen Anwendungsfall in Kraft treten soll und zu welchem Zeitpunkt es wieder deaktiviert wird.

TAF1 – Datensparsame Tarife nach § 40(5) EnWG

Datensparsame Tarife werden für Verbrauchsabrechnungen herangezogen, bei denen verhindert werden soll, dass, auf Basis der vom SMGW versandten Messwerte, Aussagen über das Verbrauchsverhalten des Letztverbrauchers gemacht werden können. Es wird nur eine Tarifstufe betrachtet.

Es ist jedoch möglich, die Zählerstände mehrerer Zähler eines Letztverbrauchers zu addieren bzw. zu subtrahieren und als Gesamtverbrauch bzw. Einspeisung zu versenden. Zu diesem Zweck übermittelt das SMGW von einem oder mehreren angeschlossenen Zählern jeweils nur einen Zählerstand pro Abrechnungszeitraum an den autorisierten externen Marktteilnehmer.

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

Notwendige Parameter für das Regelwerk:

Parameter	Beschreibung
Geräte-IDs der Zähler	Die eindeutige Bezeichnung der Zähler.
OBIS-Kennzahl der zu verwendenden Messgröße je Zähler	Die eindeutige Kennzahl der für den Tarif zu verwendenden Messgröße des jeweiligen Zählers.
Zählpunktbezeichnung	Die eindeutige Bezeichnung 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.

TAF1: Parameter

Für den jeweiligen Letztverbraucher werden an der HAN-Schnittstelle folgende Daten bereitgestellt:

- Alle Parameter des Regelwerks.
- Die Messwertliste.
- 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).

TAF2 – Zeitvariable Tarife nach § 40(5) EnWG

Bei diesem Anwendungsfall stellt der Lieferant dem Letztverbraucher für unterschiedliche Zeiträume verschiedene Preise für die in den jeweiligen Zeiträumen angefallenen Energiemengen in Rechnung. Hierzu werden im SMGW mehrere Tarifstufen definiert, an die jeweils eine Zeitbedingung geknüpft ist.
Die Zeitbedingungen der Tarifstufen werden wiederum über Tarifschaltzeitpunkte definiert. Zu jedem Zeitpunkt ist jeweils nur eine Tarifstufe aktiv.

Zum Tarifumschaltzeitpunkt erfasst das SMGW die Zählerstände von einem oder mehreren Zählern, erzeugt einen Eintrag in der Messwertliste und fügt die angefallene Energiemenge, die zwischen den beiden letzten Umschaltzeitpunkten angefallen ist, der zuletzt gültigen Tarifstufe hinzu.
Zusätzlich kann die Tarifwechselliste verschickt werden, um die Energiemengen tarifrichtig auf die zugehörigen Zeitabschnitte zu verteilen und in Rechnung zu stellen.

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

ⓘ Der Anwendungsfall ermöglicht auch die Erfassung von zeitlich variablen Einspeisungen. In diesem Fall liefert der Zähler Messwerte für eingespeiste Energiemengen. Weiterhin können Zähler für verbrauchte und eingespeiste Energiemengen auch zusammen veranlagt werden.

Notwendige Parameter für das Regelwerk:

Parameter	Beschreibung
Geräte-IDs der Zähler	Die eindeutige Bezeichnung der Zähler.
OBIS-Kennzahl der zu verwendenden Messgröße je Zähler	Die eindeutige Kennzahl der für den Tarif zu verwendenden Messgröße des jeweiligen Zählers.
Zählpunktbezeichnung	Die eindeutige Bezeichnung 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.
Gültigkeitszeitraum	Der Zeitraum, für den das Regelwerk im SMGW verwendet werden soll.

TAF2: Parameter

Für den jeweiligen Letztverbraucher werden an der HAN-Schnittstelle folgende Daten bereitgestellt:

- 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 versendeten Daten.

TAF6 – Abruf von Messwerten im Bedarfsfall

Dieser Anwendungsfall erlaubt den Abruf von Messwerten in begründeten Ausnahmefällen, wie z. B.

- den Ein- und Auszug eines Letztverbrauchers,
- einen Wechsel des Lieferanten oder
- den Wechsel in den Grundversorgungstarif.

Damit auch rückwirkende Ablesungen zu einem bestimmten Stichtag möglich sind, hält das SMGW tagesgenaue Zählerstände für jeden angeschlossenen Zähler und für jedes im SMGW vorhandene abgeleitete Register vor. Zu diesem Zweck erfasst das SMGW täglich zum Beginn des abrechnungstechnischen Kalendertages den aktuellen Zählerstand und erzeugt einen Eintrag in der Messwertliste. Messwerte, die älter als 6 Wochen sind, werden wieder aus der Messwertliste gelöscht.

Dieser Anwendungsfall ist im Hintergrund immer aktiv. Die Daten werden im begründeten Ausnahmefall im Auftrag eines externen Marktteilnehmers durch

den GWA ausgelesen und zu einem Stichtag an den externen Marktteilnehmer weitergeleitet.

ⓘ Der Grund der jeweiligen Ablesung muss für den Letztverbraucher transparent und nachvollziehbar sein.

Notwendige Parameter für das Regelwerk:

Parameter	Beschreibung
Geräte-IDs der Zähler	Die eindeutige Bezeichnung der Zähler.
OBIS-Kennzahl der zu verwendenden Messgröße je Zähler	Die eindeutige Kennzahl der für den Tarif zu verwendenden Messgröße des jeweiligen Zählers.
Zählpunktbezeichnung	Die eindeutige Bezeichnung 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.

TAF6: Parameter

Für den jeweiligen Letztverbraucher werden an der HAN-Schnittstelle folgende Daten bereitgestellt:

- 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 GWA Messwerte abgerufen hat.

TAF7 – Zählerstandsgangmessung

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.

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

Notwendige Parameter für das Regelwerk:

Parameter	Beschreibung
Geräte-ID des Zählers	Die eindeutige Bezeichnung des Zählers.
Liste von OBIS-Kennzahlen der zu registrierenden Messwerte	Die eindeutigen Kennzahlen der für den Tarif zu registrierenden Messgrößen des Zählers.
Zählpunktbezeichnung	Die eindeutige Bezeichnung 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.

TAF7: Parameter

Für den jeweiligen Letztverbraucher werden an der HAN-Schnittstelle folgende Daten bereitgestellt:

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

7.2 Wake-Up

Mit Hilfe des Wake-Up fordert der GWA das SMGW auf eine Kommunikationsverbindung herzustellen. Hierzu empfängt das SMGW vom GWA ein spezielles Datenpaket. Kann dieses vom SMGW verifiziert werden, baut es eine fest vorkonfigurierte Verbindung zum GWA auf. Dieser kann dann über den Managementkanal weitere Administrationsbefehle ausführen.

Wake-Up-Paket prüfen

Empfängt das SMGW ein Wake-Up-Paket, prüft es in der folgenden Reihenfolge ob:

- die Kennzeichnung des Paketes korrekt ist. Hierbei werden die ersten 3 Bytes des Paketes, die den Header und die Versionsnummer enthalten, geprüft.
- das SMGW der Adressat dieses Paketes ist, indem es die im Paket enthaltene Geräteidentifizierung in den Identifikationsdaten des SMGW vergleicht.
- der Zeitstempel des Wake-Up-Pakets nicht mehr als 30 Sekunden von der aktuellen Systemzeit abweicht.
- das Wake-Up-Paket nicht schon einmal empfangen wurde.
- die Signatur des Pakets vom GWA stammt.

Konnten Teile des Wake-Up-Pakets nicht durch das SMGW verifiziert werden, d. h. die Überprüfung der Kennzeichnung, der Geräteidentifizierung, des Zeitstempels oder der Signatur ist fehlerhaft, wird die Prüfung beim ersten Fehler unterbrochen und die Nachricht sofort verworfen. Es wird keine Verbindung zum Absender des Paketes aufgenommen.

Wurde das Wake-Up-Paket erfolgreich verifiziert, so wird die Nachricht verworfen und ein TLS-Kanal zum GWA aufgebaut. Die Adressierungsdaten hierfür sind im SMGW vorkonfiguriert.

ⓘ Die Sicherheitsfunktionen des SMGW verhindern, dass das gleiche Wake-Up-Paket ein weiteres Mal genutzt werden kann.

8 Sichere Entsorgung

Hardwareentsorgung

Komponenten	Abfallsammlung und Entsorgung
Leiterplatten	Elektronikabfall: Entsorgung gemäß den örtlichen Vorschriften.
Metallteile	Wertstoff, wiederverwertbar: nach Sorten getrennt in Metallcontainern sammeln.
Kunststoffteile	Nach Sorten getrennt der Wiederverwertung (Regranulierung) zuführen. Ggf. der Müllverbrennung zuführen (Energiegewinnung durch thermische Verfahren).

9 Anhang

9.1 Abkürzungsverzeichnis

A

AES *Advanced Encryption Standard*

B

BSI *Bundesamt für Sicherheit in der Informationstechnik*

C

CLS *Controllable Local Systems*
CMS *Cryptographic Message Syntax*
CRC *Cyclic Redundancy Check*

E

EMT *Externer Marktteilnehmer*
ERP *Enterprise Resource Planning*

G

GSM *Global System for Mobile*

H

HAN *Home Area Network*

L

LMC *Local Meter Controller*

P

PRF *Pseudorandom Function*
PWR *Power*

S

SMGW *Smart Meter Gateway*

T

TLS *Transport Layer Security*

U

UMTS *Universal Mobile Telecommunications System*

W

WAN *Wide Area Network*
wMT *wireless MBus-Traffic*