Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Technische Richtlinie BSI TR-03109-1

Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems

Version 2.0

13.12.2024

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: smartmeter@bsi.bund.de
Internet: https://www.bsi.bund.de
© Bundesamt für Sicherheit in der Informationstechnik 2024

Inhalt

1 Einleitung 1
1.1 Vorwort 1
1.2 Zielsetzung 2
1.3 Zielgruppe 2
1.4 Anwendungsbereich 2
1.5 Fachlich zuständige Stelle 2
1.6 Terminologie 2
1.7 Aufbau der Technischen Richtlinie 3
1.8 Übersicht über mitgeltende Anlagen 3
1.9 Zusammenhang mit anderen Technischen Richtlinien 4
1.10 Nachweispflicht zur Interoperabilität nach MsbG 4
1.11 Versionshistorie 5

2 Technische Einleitung 6
2.1 Einleitung 6
2.2 Akteure am SMGW 6
2.3 Schnittstellen und Funktionen des SMGW 7
2.4 Interoperabilitätsmodell 12
2.5 Fachliche Anwendungsfälle und FA-Kategorien 14
2.6 Datenstrukturen und Profile 20

3 Funktionale Anforderungen an das SMGW 24
3.1 Einleitung 24
3.2 Verarbeitung von abrechnungsrelevanten Messwerten (FAKAT.ValProcBilling) 25
3.3 Verarbeitung von nicht-abrechnungsrelevanten Messwerten (FAKAT.ValProcNonBilling) 45
3.4 Versand von Messwerten im WAN (FAKAT.ValTransmission) 49
3.5 Erfassung von Messwerten (FAKAT.ValCapture) 58
3.6 Dienste für lokale Nutzer (FAKAT.ConServices) 66
3.7 CLS-Dienste und Proxy-Funktionen (FAKAT.ClsServices) 79
3.8 Dienste für den Servicetechniker im HAN (FAKAT.SrvServices) 85
3.9 Erweiterte Dienste für Messeinrichtungen im LMN (FAKAT.MtrServices) 87
3.10 Zeitführung des SMGW (FAKAT.SmgwTimeSync) 91
3.11 Anbindung von Messeinrichtungen im LMN administrieren (FAKAT.LmnComConfig) 98
3.12 Anbindung von EMT administrieren (FAKAT.EmtComConfig) 105
3.13 Anbindung von HAN-Teilnehmern administrieren (FAKAT.HanUserConfig) 106
3.14 Messwertverarbeitung administrieren (FAKAT.ValProcConfig) 113
3.15 Proxy-Kommunikation administrieren (FAKAT.ProxyConfig) 120
3.16 Monitoring und Diagnose des SMGW (FAKAT.SmgwMonitoring) 124
3.17 Administrationsvoraussetzungen herstellen und erhalten (FAKAT.SmgwAdministration) 135
3.18 GWA-Wechsel (FAKAT.GwaSwitch) 149
3.19 Verwaltung der SMGW-Zertifikate (FAKAT.SmgwCertMgmt) 151
3.20 Firmware Download und Update (FAKAT.SmgwFwUpdate) 163
3.21 Netzwerkdiagnose (FAKAT.NetworkDiagnosis) 168

3.22 Datenstrukturen und Profile 175

4 Anforderungen an die Kommunikationsverbindungen und Protokolle des SMGW 233
4.1 Einleitung 233
4.2 Kommunikation des SMGW im WAN 234
4.3 Kommunikation des SMGW im LMN 256
4.4 Kommunikation des SMGW im HAN 265

5 Nicht-Funktionale Anforderungen 286
5.1 Einleitung 286
5.2 Versiegelung 286
5.3 Eindeutige Geräte-Identifikation des SMGW 286
5.4 Einbau des Sicherheitsmoduls 286
5.5 Vorhaltefristen 286
5.6 Mindestanforderungen an die Leistungsfähigkeit 287
5.7 Protokollierung IT-sicherheitsrelevanter Ereignisse 288

Literaturverzeichnis 297

Glossar 300

A Tabelle der zu protokollierenden Ereignisse 303

B Abkürzungsverzeichnis 324

C Lokale Zugriffsrechte 326

D Anwenderhinweise für den MSB 331

E Changelog 334

Anforderungsverzeichnis 343

ICS-Verzeichnis 369

Abbildungsverzeichnis

2.1. Einbettung des SMGW in seine Einsatzumgebung 8
2.2. Interoperabilitäts-Modell der Technischen Richtlinie 13
3.1. Funktionsblöcke des SMGW 24
3.2. Ablauf der Messwertverarbeitung für abrechnungsrelevante und historische Messwerte 26
3.3. Beispiel für Ableitung des Lastgangs und Bestimmung des Leistungsmaximalwerts 36
3.4. Beispiel für einen zeitvariablen Tarif mit zwei Tarifstufen (HT/NT) 40
3.5. Ablaufdiagramm für TAF2 41
3.6. Ablauf der Messwertverarbeitung für Netzzustandsdaten und Momentanwerte 45
3.7. Verhalten bei Über- oder Unterschreitung von Schwellwerten mit Hysterese 54
3.8. Ablauf der verschiedenen Versandauslösebedingungen 54
3.9. Legende und Zeichenerklärung für die folgenden Grafiken 59
3.10. Zeitlicher Zusammenhang von Messung, Abfrage und Erfassung über LKS1 61
3.11. Zeitlicher Zusammenhang von Messung und Erfassung von Einzelwerten über LKS2 63
3.12. Zeitlicher Zusammenhang von Messung, Bündelversand und Erfassung über LKS2 64
3.13. Proxy-Funktion zwischen CLS und EMT 79
3.14. Transparenter Kommunikationskanal initiiert durch CLS 81
3.15. Synchronisations-Hierarchie des Intelligenten Messsystems 92
3.16. Ablaufdiagramm einer Zeitsynchronisation 94
3.17. Status der Systemzeit bei verschiedenen Ereignissen 94
3.18. Relationen zwischen Entitäten der Messwertverarbeitung des SMGW 113
3.19. Übersicht über den Ablauf der GWA-Authentifizierung am Sicherheitsmodul des SMGW 145
3.20. Schlüssel- und Zertifikatsverarbeitung beim Erstellen neuer SMGW-PKI-Zertifikate 155
3.21. Übersicht der verwendeten Kommunikationsszenarien 169
3.22. Beispiel verschiedener Versandzeitpunkte im zeitlichen Verlauf 171
4.1. Lebensdauer von TLS-Session, TLS-Verbindung und HTTP-Nachrichtenaustausch 233
4.2. Protokollstapel für die WAN-Kommunikationsszenarien 236
4.3. Übersicht über den Ablauf des WKS.MANAGEMENT 239
4.4. Übersicht über den Ablauf des WKS.ADMIN-SERVICE 242
4.5. Übersicht über den Ablauf des WKS.INFO-REPORT zum EMT 245
4.6. Übersicht über den Ablauf des WKS.INFO-REPORT via GWA 246

4.7. Übersicht über den Ablauf des WKS.NTP-TLS 249
4.8. Übersicht über den Ablauf des WKS.TLSPROXY 251
4.9. Übersicht der Interaktion zwischen WKS.WAKEUP und WKS.MANAGEMENT 252
4.10. Übersicht über den Ablauf des WKS.DOWNLOAD 255
4.11. Protokollstapel im LMN (für drahtlose und drahtgebundene Kommunikation) 257
4.12. Übersicht über den Protokollstapel von LKS1 259
4.13. Übersicht über den Ablauf des LKS1.TLS 259
4.14. Übersicht über den Protokollstapel von LKS1.PSK 262
4.15. Übersicht über den Ablauf des LKS1.PSK 262
4.16. Übersicht über den Protokollstapel des LKS2 264
4.17. Sequenzdiagramm für unidirektionale LMN-Kommunikation (LKS2) 264
4.18. Protokollstapel für die HAN-Kommunikation 267
4.19. Authentifizierung des Nutzers im HAN mittels TLS-Client-Zertifikat 271
4.20. Authentifizierung des Anschlussnutzers im HAN mittels Nutzerkennung und Passwort 274
4.21. Übersicht über den Ablauf des HKS.TLSPROXY.SOCKS (1/2) 276
4.22. Übersicht über den Ablauf des HKS.TLSPROXY.SOCKS (2/2) 277
4.23. Übersicht über den Ablauf des HKS.TLSPROXY.SRV 279
4.24. Übersicht über den Ablauf des HKS.TLSPROXY.CLI 281
4.25. Übersicht über den Ablauf des HKS.NTP-TLS.SRV 283
4.26. Übersicht über den Ablauf der automatischen Adressbestimmung im HAN 284
C.1. Ablauf der Berechtigungsprüfung beim lokalen Zugriff auf Ressourcen des SMGW 327
C.2. Übersicht über die Attribut-basierte Berechtigungskontrolle beim lokalen Zugriff auf Ressourcen des SMGW 328

1 Einleitung

1.1 Vorwort

Die mit der rasanten Technologieentwicklung einhergehende Digitalisierung aller gesellschaftlichen Lebensbereiche stellt Staat, Wirtschaft und unsere Gesellschaft vor große Herausforderungen. Die Energiewende ermöglicht Bürgerinnen und Bürgern hohen Einfluss auf das eigene Verbrauchsverhalten und die direkte Teilnahme am Energiemarkt. Eigene Erzeugung, die Nutzung dynamischer Tarife oder die Teilnahme an Mieterstrommodellen ermöglicht direkte Kostenersparnisse für Bürgerinnen und Bürger.

Netzseitig müssen hierdurch anstelle von wenigen Großkraftwerken eine Vielzahl von kleinen, dezentralen *Erzeugungsanlagen*, Anlagen zur Speicherung elektrischer Energie und flexiblen Verbrauchseinrichtungen in das intelligente Energienetz integriert werden. Weiterhin werden auch auf Verbraucherseite durch den Hochlauf der Elektromobilität sowie die Wärmewende steuerbare und flexible Kundeneinrichtungen entstehen. Flexibilität im zukünftigen Smart Grid ist nötig, um Erzeugung und *Verbrauch* aufeinander abzustimmen.

Die Integration dieser steuerbaren Erzeugungs- und Verbrauchseinrichtungen ist essenziell für das Gelingen der Energiewende und muss cybersicher erfolgen. Die Bedrohung im Cyberraum ist so hoch wie nie zuvor. Auch die Energieinfrastruktur muss resilient sein und auch geopolitischen Spannungen widerstehen.

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

SMGW als zentrale Kommunikationseinheiten gewährleisten Datenschutz und Datensicherheit auf höchstem Niveau („Security & Privacy by Design“). Im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) entwickelt das BSI daher Anforderungen an vertrauenswürdige Produktkomponenten (SMGW mit integriertem Sicherheitsmodul, Kommunikationsadapter), deren sicheren IT-Betrieb (Administration) und an die vertrauenswürdige Kommunikationsinfrastruktur (Smart-Metering-Public-Key-Infrastruktur) in Form von Schutzprofilen und Technischen Richtlinien.

Mit dem Gesetz zum Neustart der Digitalisierung der Energiewende (GNDEW) hat der Gesetzgeber die Kompetenzen des BSI geschärft und insbesondere klargestellt, dass die Schnittstellenspezifikation des SMGW einschließlich Anwendungsprogrammierschnittstellen sowie der Kommunikationsverbindungen, Datenstrukturen, Prozesse und Protokolle durch das BSI zu beschreiben ist.

Mit der nun vorliegenden Version 2.0 der Technischen Richtlinie TR-03109-1 trägt das BSI den sich verändernden Anforderungen des Marktes Rechnung und erzielt u.a. durch die folgenden wesentlichen Änderungen erhebliche Vorteile bei der Verwendung von SMGW:

- Durch eine Vereinheitlichung der WAN-API sowie die Einführung einer verbindlichen HAN-API werden SMGW künftig an den Schnittstellen austauschbar (Interchangeability). Für Betreiber von SMGW werden dadurch Integrations- und Wechselprozesse erheblich vereinfacht und insgesamt wirtschaftlicher. Anschlussnutzer können künftig über eine einheitliche Schnittstelle auf ihre Daten zugreifen und diese lokal und in Echtzeit z.B. in bestehende Smart-Home-Lösungen integrieren.
- Erweiterte Rechte für den Servicetechniker sowie Funktionen zum Werksreset ermöglichen eine effiziente Entstörung von SMGW bis hin zum Ausbau zur Wiederverwendung.
- Erweiterungen für Multispartenmetering ermöglichen die Erfassung von Messwerten der Sparten Elektrizität, Gas, Wasser und Thermische Energie über die LMN-Schnittstelle des SMGW, zudem werden Anwendungsfälle für Submetering für Elektrizität-, Gas-, und Wärmemengenzähler eichrechtskonform, interoperabel und verbraucherfreundlich über LMN möglich.

Eine detaillierte Auflistung der Änderungen findet sich in ▸Anhang E.

1.2 Zielsetzung

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

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

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

1.3 Zielgruppe

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

1.4 Anwendungsbereich

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

1.5 Fachlich zuständige Stelle

Fachlich zuständig für die Fortentwicklung der TR ist das BSI.

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

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

1.6 Terminologie

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

- **MUSS / MÜSSEN** bedeutet, dass es sich um eine normative Anforderung handelt.
- **MUSS+** bezeichnet eine Anforderung, die spätestens ab dem 01.01.2027 normativ umzusetzen ist.
- **DARF NICHT / DARF KEIN / DÜRFEN NICHT / DÜRFEN KEIN** bezeichnet den normativen Ausschluss einer Eigenschaft.
- **SOLL / SOLLEN** beschreibt eine dringende Empfehlung. Abweichungen zu diesen Festlegungen müssen begründet werden.
- **KANN / KÖNNEN / DARF / DÜRFEN** bedeutet, dass die Eigenschaften fakultativ oder optional sind.

Die Anforderungen der Technischen Richtlinie sind grundsätzlich als normativ anzusehen. In Abhängigkeit von den Anforderungen des Marktes können künftig SOLL-Anforderungen verpflichtend werden, um die Interoperabilität des Gesamtsystems zu erhöhen und zu stabilisieren.

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

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

Tabelle 1.1 Anforderungstypen

1.7 Aufbau der Technischen Richtlinie

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

Kapitel ▸3 enthält die funktionalen Anforderungen an das SMGW in Form von Fachlichen Anwendungsfällen, die in FA-Kategorien einsortiert sind.

Das folgende Kapitel ▸4 macht Vorgaben zur Sicherung aller Kommunikationsbeziehungen des SMGW und stellt Mindestanforderungen an die *Kommunikationsszenarien* und Protokolle in Bezug auf die zu unterstützenden Anwendungsfälle.

Nicht-funktionale Anforderungen bzw. Eigenschaften, die das SMGW zusätzlich aufweisen muss, finden sich in Kapitel ▸5.



Anmerkung

Mit dieser Version der TR wurde eine grundlegende Umstrukturierung vollzogen. Die bisherige Darstellung der Anforderungen weicht einer anwendungsfallorientierten Beschreibung (in FA). Hierdurch entsteht eine größere Flexibilität bei der Wartung und Weiterentwicklung der TR, die sich zudem deutlich implementierungsnäher gibt und damit der ▸Zielgruppe besser gerecht wird.

1.8 Übersicht über mitgeltende Anlagen

- Die Detailspezifikationen zur TR-03109-1 [DS] regeln Details der Implementierung, beispielsweise zur Struktur des Wake-Up-Pakets und der Zertifikatsprofile und schließen Interpretationslücken in referenzierten Universalspezifikationen. Normative Anforderungen sind in den Detailspezifikationen entsprechend der Vorgaben dieser TR mit eindeutigen Bezeichnern gekennzeichnet.
- Die Anlage I: CMS-Datenformat für die Inhaltsdatenverschlüsselung und -signatur ist entfallen. Sie wurde durch das Kapitel "CMS" der Detailspezifikation zur TR-03109-1 ersetzt.
- Die Anlage II: COSEM/HTTP Webservices ist entfallen. An ihre Stelle tritt das Kapitel "RESTful Webservice" der Detailspezifikation zur TR-03109-1 und die **normative** "Anlage Webservice-APIs des SMGW".

- Die Anlage IIIa: Feinspezifikation "Drahtlose LMN-Schnittstelle" Teil a: "OMS Specification Volume 2, Primary Communication" ist entfallen. Sie wurde durch das Kapitel "Wireless MBUS" der Detailspezifikation zur TR-03109-1 ersetzt.
- Die Anlage IIIb: Feinspezifikation "Drahtlose LMN-Schnittstelle" Teil b: "OMS Technical Report Security" ist entfallen. Sie wurde durch Kapitel "Wireless MBUS" der Detailspezifikation zur TR-03109-1 ersetzt.
- Die Anlage IVa: Feinspezifikation "Drahtgebundene LMN-Schnittstelle" Teil a: "HDLC für LMN" ist entfallen. Sie wurde durch Kapitel "Bidirektionale LMN-Kommunikation über HDLC" der Detailspezifikation zur TR-03109-1 ersetzt.
- Die Anlage IVb: Feinspezifikation "Drahtgebundene LMN-Schnittstelle" Teil b: "SML – Smart Message Language" ist entfallen. An den relevanten Stellen wurde stattdessen ein Verweis auf [VDE0418-63-9] eingefügt.
- Die Anlage V: Anforderungen zum Betrieb beim Administrator ist entfallen. Die dortigen Anforderungen wurden in die Richtlinie [TR-03109-6] überführt.
- Die Anlage VI: Betriebsprozesse [TR-03109-1-VI] ist **informativ** und beschreibt die vorgesehene Verwendung des SMGW. Die Anlage wurde im Zuge dieses Releases ebenfalls grundlegend überarbeitet.
- Die Anlage VII: Interoperabilitätsmodell und Geräteprofile für Smart-Meter-Gateways ist entfallen. Die dortigen Anforderungen wurden in die TR-03109-1 überführt.
- Die Anlage VIII: Lebenszyklus [TR-03109-1-VIII] ist **informativ** und beschreibt den Lebenszyklus von der Entwicklung bis zur Verschrottung.
- Auf der BSI-Homepage veröffentlichte Implementierungshinweise zur TR-03109-1 schließen Interpretationslücken in der TR, geben "best practice"-Hinweise zur Umsetzung bestimmter Dienste oder Details. Es handelt sich um nicht-verbindliche Dokumente, die die Sichtweise bzw. Interpretation des BSI aufzeigen und keinen direkten Einfluss auf die TR haben, auf die sie sich beziehen.

  Implementierungshinweise dienen darüber hinaus zur Veröffentlichung von Spezifikationen für eine herstellerübergreifende Interoperabilität zur Erprobung innovativer Dienste oder Anwendungsfälle des SMGW.

1.9 Zusammenhang mit anderen Technischen Richtlinien

- Die Richtlinie [TR-03109-2] beschreibt das Sicherheitsmodul des SMGW und die von ihm bereitzustellende Funktionalität.
- Die Richtlinie [TR-03109-3] legt Vorgaben an die einzusetzenden kryptographischen Verfahren fest.
- Die Richtlinie [TR-03109-4] spezifiziert die Architektur sowie die Mindestanforderungen an Interoperabilität und Sicherheit der Smart-Metering-PKI (SM-PKI).
- Die Richtlinie [TR-03109-5] beschreibt Mindestanforderungen an Kommunikationsadapter im HAN des SMGW für Hersteller von *CLS*.
- Die Richtlinie [TR-03109-6] beschreibt die Anforderungen an den Smart-Meter-Gateway-Administrator (GWA).

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

1.10 Nachweispflicht zur Interoperabilität nach MsbG

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

1.11 Versionshistorie

Version	Datum	Beschreibung
0.20	10.10.2011	Veröffentlichung Draft 1
0.50	25.05.2012	Veröffentlichung Draft 2
1.0 RC	21.12.2012	Veröffentlichung Version 1.0 (Release Candidate)
1.0	18.03.2013	Veröffentlichung Version 1.0
1.0.1	16.01.2019	Veröffentlichung Version 1.0.1 - Anlage VII ergänzt
1.1	17.09.2021	finale Version nach Abstimmung im Ausschuss Gateway-Standardisierung, Grundlegende Überarbeitung zur Vorversion.
2.0	13.12.2024	finale Version nach Abstimmung im Ausschuss Gateway-Standardisierung. Changelog s. ▸Anhang E

Tabelle 1.2 Versionshistorie

2 Technische Einleitung

2.1 Einleitung

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

Des Weiteren beschreibt dieses Kapitel die mit dem SMGW kommunizierenden Akteure (▸Abschnitt 2.2).

2.2 Akteure am SMGW

2.2.1 Einleitung

Zur Beschreibung der Funktionalität des SMGW ist es erforderlich, verschiedene Akteure zu benennen, die im Kontext dieser Technischen Richtlinie mit dem SMGW kommunizieren. Die Notwendigkeit und Definition jedes Akteurs ergibt sich dabei entweder direkt aus dem Rechtsrahmen oder als technische Notwendigkeit zur Erfüllung von Anwendungsfällen, die durch den Rechtsrahmen gefordert werden. Die hier definierten Akteure sind im Rahmen des SMGW-Betriebs relevant. In anderen Phasen des Lebenszyklus können weitere Rollen involviert sein. Diese werden in der entsprechenden Anlage zum Lebenszyklus benannt [TR-03109-1-VIII].

Die folgenden Abschnitte beschreiben die Akteure des SMGW.

2.2.2 Anschlussnutzer

Akteur am SMGW, der elektrische Energie, thermische Energie, Gas oder Wasser bezieht oder erzeugt und zur Nutzung des Netzanschlusses berechtigt ist. Der Begriff Anschlussnutzer umfasst auch die Bezeichnungen Letztverbraucher, Endkunde und Anlagenbetreiber die in [EEG], [EnWG], [MsbG] genannt werden. Für diese Akteure wird in dieser TR die Rolle des lokalen Nutzers "CON" verwendet. Der Anschlussnutzer nutzt zur Kommunikation mit dem SMGW eine Komponente, die die Anwendungsprogrammierschnittstelle (API) im Home Area Network (HAN) des SMGW verwendet. Die Komponente ist beispielsweise ein PC mit Browser oder Transparenz-Software, ein Display, ein Energie-Management-System (EMS) oder eine Heimautomatisierungskomponenten. In früheren Versionen dieses Dokuments wurde und in referenzierten Dokumenten wird der Anschlussnutzer auch als Letztverbraucher bezeichnet. Gleiches gilt für Kompositionen wie dem Letztverbraucher-Log.

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

2.2.3 Smart-Meter-Gateway-Administrator

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

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

Das Kommunikationssystem des GWA nutzt die WAN-API des SMGW für die Rolle GWA.

2.2.4 Berechtigte Externe Marktteilnehmer (External Market Participant)

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

Berechtigte EMT werden in der SM-PKI Policy [SM-PKI-CP] weiter differenziert in passive EMT, die den TLS-Proxy nicht nutzen dürfen und Daten nur vom SMGW empfangen und aktive EMT, die über den TLS-Proxy des SMGW Informationen mit nachgelagerten Geräten (Controllable Local Systems) austauschen und auf diese einwirken dürfen.

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

Das SMGW nutzt für die Messwertübertragung die WAN-API des EMT.

2.2.5 Messeinrichtungen

Messeinrichtungen (eng. Meter, MTR) im Local Metrological Network (LMN) dienen der Erfassung von *Verbrauch* und Erzeugung von *Stoff- oder Energiemengen*. Erhobene *Messwerte* werden von der Messeinrichtung an das SMGW übermittelt. In diesem Dokument wird der Begriff *Zähler* synonym zu *Messeinrichtung* verwendet.

2.2.6 Steuerbare lokale Systeme (Controllable Local Systems)

Controllable Local Systems (CLS) sind Systeme mit IT-Komponenten an der HAN-Schnittstelle des SMGW, die nicht zum Intelligenten Messsystem gehören, aber das SMGW für bestimmte Kommunikationszwecke verwenden. CLS können von lokalen *Erzeugungsanlagen* über steuerbare Lasten wie Wärmepumpen, Ladegeräte für Elektrofahrzeuge oder Batteriespeicher bis hin zu Anwendungen in der Hausautomation reichen. Darüber hinaus werden Geräte für Mehrwertdienste unter dem Begriff CLS zusammengefasst. Ein CLS nutzt die HAN-Anwendungsprogrammierschnittstelle (API) für die Rolle CLS.

2.2.7 Servicetechniker

Der Servicetechniker (SRV) des GWA kann am Einsatzort des SMGW im Wirkbetrieb eine lokale Diagnoseschnittstelle am SMGW nutzen, um lesenden Zugriff auf das System-Logbuch und weitere Diagnosedaten zu erhalten sowie das Gerät in engen Grenzen zu parametrieren. SRV kann sowohl die Person als auch das von der Person verwendete Komponente (z.B. Diagnosegerät) bezeichnen. Die Komponente des Service-Technikers nutzt die HAN-Anwendungsprogrammierschnittstelle (API) für die Rolle SRV.

2.3 Schnittstellen und Funktionen des SMGW

2.3.1 Einleitung

Abgeleitet von der Systemarchitektur, die auf den Vorgaben des Schutzprofils [PP-0073] beruht, kommuniziert ein SMGW über verschiedene Netzwerke und Schnittstellen, wie in ▸Abbildung 2.1 dargestellt.

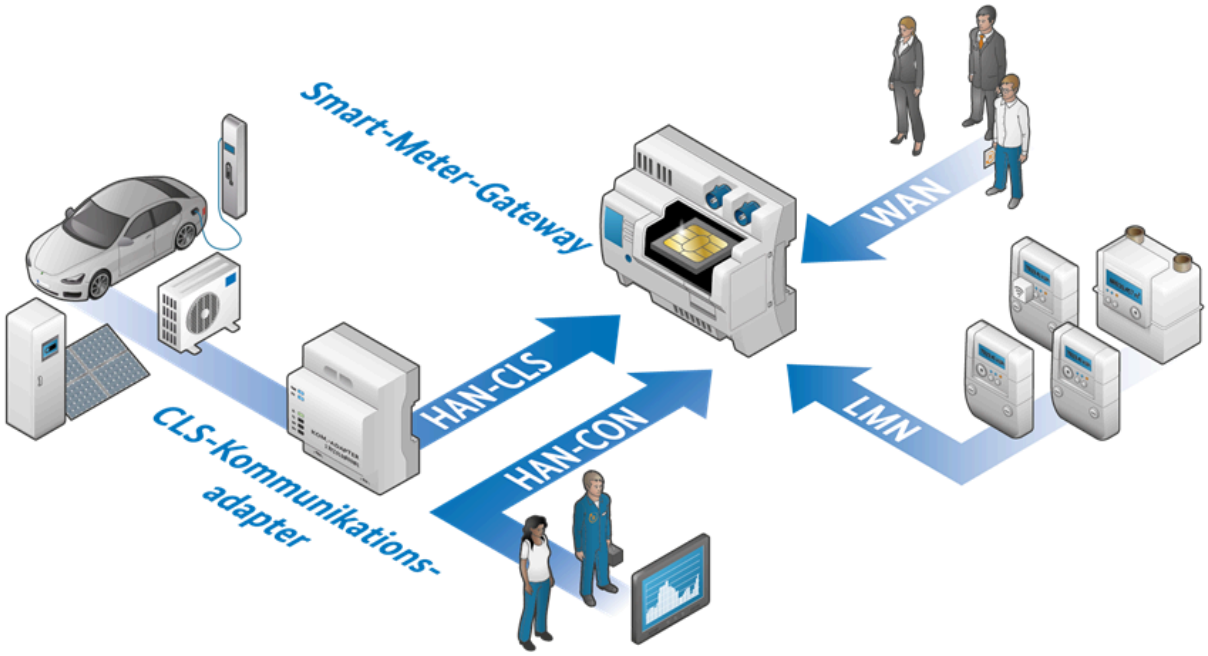


Abbildung 2.1. Einbettung des SMGW in seine Einsatzumgebung

Folgende Kommunikationsbereiche werden betrachtet:

- **Lokales metrologisches Netz (Local Metrological Network, LMN)**: Im LMN kommuniziert das SMGW mit den angebundenen Messeinrichtungen für Stoff- und Energiemengen (Gas, Wasser, thermische Energie und Elektrizität) eines oder mehrerer Anschlussnutzer. Die Messeinrichtungen sind über eine von zwei physischen LMN-Schnittstellen an das SMGW angebunden: Im bedrahteten LMN kommuniziert die Messeinrichtung bidirektional mit dem SMGW. Im drahtlosen LMN kommunizieren die Messeinrichtungen mittels Nahfeldfunkkommunikation (Wireless M-Bus) unidirektional mit dem SMGW.
- **Weitverkehrsnetz (Wide Area Network, WAN)**: Im WAN kommuniziert das SMGW - durch die SM-PKI gesichert - mit dem GWA und den EMT.
- **Heimnetz (Home Area Network, HAN)**: Im HAN kommuniziert das SMGW mit lokalen Kommunikationspartnern. Dies sind Kommunikationsadapter und Steuerungseinrichtungen für steuerbare Energieverbrauchs- und -erzeugungseinrichtungen (z.B. Netzwirksame Wärmepumpen, Klimageräte, Energiespeicher, Photovoltaikanlagen, Ladeeinrichtungen für E-Fahrzeuge und EMS) und auch Ausstattungen zur Verbrauchserfassung (Datenkonzentratoren für Heizkostenverteiler) oder weitere Mehrwertdienste mit der Rolle CLS. Das SMGW stellt über die HAN-Schnittstelle für CLS, Endkunden (Anschlussnutzer und Anlagenbetreiber mit der Rolle CON) und Service-Techniker (Rolle SRV) seine Dienste bereit.

  Zur Erhöhung des Schutzes der CLS wird eine Trennung des HAN in zwei Netzwerke HAN-CON und HAN-CLS empfohlen.

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

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

Daneben bietet das SMGW Funktionen für Anschlussnutzer bzw. Servicetechniker. Anschlussnutzer können an der HAN-Schnittstelle Verbrauchsdaten abrufen, Servicetechniker können Systeminformationen abrufen. Für im HAN angeschlossene steuerbare Systeme (CLS) fungiert das SMGW als TLS-Proxy-Server: TLS-

geschützte Kommunikationskanäle in Richtung CLS und in Richtung EMT werden im SMGW terminiert und das SMGW übernimmt die Weiterleitung der jeweils empfangenen Daten.

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

2.3.2 Funktionen des SMGW für das lokale metrologische Netz

Das SMGW kommuniziert mit *Zählern* im lokalen metrologischen Netz und ist für den Empfang, die Verarbeitung und Speicherung von Messwerten und ggf. Netzzustandsdaten verantwortlich. Die lokal angebundenen Zähler werden dem SMGW in Form von entsprechenden *LMN-Kommunikationsprofilen* durch den GWA bekannt gemacht (▸Abschnitt 3.22.25).

Die sichere Kommunikation mit den Zählern erfolgt mit Hilfe der in ▸Abschnitt 4.3 festgelegten Protokolle.

Erfassung, Zeitstempelung, Tarifierung und Speicherung von Messwerten

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

1. Das SMGW empfängt oder ruft in regelmäßigen Zeitabständen die Messwerte der lokal angeschlossenen Zähler ab. Das SMGW empfängt die Messwerte verschlüsselt und integritätsgesichert.
2. Das SMGW führt die Zeitstempelung empfangener Messwerte mithilfe der Systemuhr durch und speichert die Messwerte nach erfolgreicher Entschlüsselung und Integritätsprüfung in *Messwertlisten*.
3. Mit Hilfe eines *Regelwerks* bestimmt das SMGW die an berechtigte EMT zu versendenden Messwerte.

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

Diese Technische Richtlinie beschreibt weitere Dienste, die ein SMGW angeschlossenen Messeinrichtungen anbieten muss oder soll:

- Einen Schlüsselerzeugungs- und Zertifikatserneuerungsdienst
- Die Bereitstellung der mit der gesetzlichen Zeit synchronisierten Systemzeit
- Dateiübertragungsdienste für Firmware und Parameterkonfiguration
- Abruf von Dateien aus der Messeinrichtung (Logbuch, Netzqualitätsmesswerten (Power Quality) gemäß DIN EN 50160

2.3.3 Funktionen des SMGW für das Weitverkehrsnetz

Die Verbindung des SMGW zum GWA sowie zu den EMT geschieht über eine WAN-Verbindung, die über Zertifikate der SM-PKI gesichert ist.

Die Kommunikation erfolgt mittels der in ▸Abschnitt 4.2 festgelegten Protokolle.

Der GWA ist die vertrauenswürdige Instanz im WAN, die das SMGW konfiguriert, administriert, den ordnungsgemäßen Betrieb überwacht und den zuverlässigen technischen Betrieb gewährleistet. Zu den Aufgaben des GWA siehe [TR-03109-1-VI] Kapitel Betriebsprozesse GWA. Die Vertrauenswürdigkeit wird durch die Zertifizierung seines ISMS gemäß [TR-03109-6] gewährleistet.

Übertragung der Messwerte anhand von Auswertungs- und *WAN-Kommunikationsprofilen*

Im SMGW werden vom GWA Regelwerke in Form von *Auswertungsprofilen* hinterlegt (▸Abschnitt 3.22.6 dieses Dokuments und in [PP-0073]), die die Weiterverarbeitung der empfangenen Informationen beschreiben.

Nach der Verarbeitung erfolgt die Auslieferung der Daten an berechtigte EMT im WAN und nach Ablauf der erforderlichen Aufbewahrungszeiten deren Löschung. Die Verbindungsparameter für die Übertragung der Messwerte hat das SMGW in *Kommunikationsprofilen* gespeichert.

Pseudonymisierung

Das SMGW unterstützt die Pseudonymisierung der Identifikation eines dem Anschlussnutzer zugeordneten Zählers, sofern die Identifikation nicht für berechtigte Zwecke benötigt wird. Damit auch die Identität des sendenden SMGW unerkannt bleibt, müssen die Daten zusätzlich über einen Dritten (den GWA) an den Endempfänger vermittelt werden.

Empfang von Administrations- und Konfigurationsinformationen

Das SMGW wird vom GWA konfiguriert und administriert. Dazu sendet der GWA Konfigurationsinformationen und Befehle, die vom SMGW empfangen und verarbeiten werden. Datenstrukturen zur Konfiguration mit einer definierten Semantik werden in dieser Technischen Richtlinie als "Konfigurationsprofile" bezeichnet.

Firmware-Update

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

Wake-Up-Service

Das SMGW stellt einen Wake-Up-Service für den GWA bereit (Siehe ▸FA.InitiateManagementConnection). Der GWA kann mithilfe des Wake-Up-Service das SMGW auffordern eine WAN-Kommunikationsverbindung aufzubauen. Beim Wake-Up-Service empfängt das SMGW ein spezielles vom GWA signiertes Datenpaket. Nach erfolgreicher Verifikation dieses einzelnen Paketes baut das SMGW eine durch den GWA vorkonfigurierte Verbindung auf.

Zeitsynchronisation

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

Die Synchronisation der SMGW-Systemuhr mit einer zuverlässigen externen Zeitquelle geschieht gemäß den Vorgaben aus ▸FAKAT.SmgwTimeSync.

2.3.4 Funktionen und Dienste des SMGW für lokale Nutzer im HAN

Der GWA legt die Rolle (CON, CLS, SRV) der identifizierten und authentifizierten HAN-Teilnehmer über ein HAN- oder Proxy-Kommunikationsprofil im SMGW fest. Gemäß HAN-Berechtigung (Siehe ▸Anhang C) kann der über eine TLS-gesicherte Verbindung authentifizierte lokale Nutzer verschiedene Dienste des SMGW nutzen.

Die sichere Kommunikation mit den HAN-Teilnehmern erfolgt mit Hilfe der in ▸Abschnitt 4.4 festgelegten Protokolle.

CLS - Controllable Local System

Diese Technische Richtlinie beschreibt Dienste und Informationen, die ein SMGW lokalen Nutzern mit der Rolle CLS bereitstellen soll oder muss:

- den TLS-Proxy-Dienst zur Nutzung eines sicheren Kommunikationskanals mit einem vom GWA konfigurierten aktiven EMT [1],
- die mit der gesetzlichen Zeit synchronisierte Systemzeit des SMGW,
- Historische und aktuelle Messwerte der dem CLS zugeordneten Messeinrichtungen,
- einen Schlüsselerzeugungs- und Zertifikatserneuerungsdienst,

[1] Das SMGW vermittelt die Daten des sicheren Kommunikationskanals, verarbeitet und speichert diese jedoch nicht selbst

- Statusinformationen zur Zertifikatsgültigkeit und dem Zustand des TLS-Proxy-Kanals.

CON - Consumer (Endkunde)

Das SMGW soll oder muss für lokale Letztverbraucher, Anschlussnutzer, Anschlussnehmer, Anlagenbetreiber oder Endkunden mit der Rolle CON die folgenden Dienste und Informationen bereitstellen:

- das dem Endkunden zugeordnete Anschlussnutzer-Logbuch mit Transparenzinformationen,
- die mit der gesetzlichen Zeit synchronisierte Systemzeit des SMGW,
- aktuelle Zählerstände und Messwerte,
- historische Zählerstände und Verbrauchsinformationen,
- Informationen zum aktuellen Tarif (Tarifstufen, Zähleridentifikation, EMT-Identifikation, Regelwerkparameter).

Zur Auslesung und Visualisierung der Daten kann beispielsweise eine einfache Verbrauchsanzeige, ein lokaler PC mit der Transparenz- und Displaysoftware als Sichtanzeige nach [MessEG]/[MessEV] oder auch ein anderes Gerät des Endkunden genutzt werden.

SRV - Service Techniker

Das SMGW soll oder muss für die vom GWA autorisierten Service-Techniker (Rolle SRV) folgende Dienste und Informationen bereitstellen:

- Abruf des Syslog mit Ereignissen zur kommunikativen Anbindung, Anomalien und Fehlern,
- Abruf des Eichlogs,
- Abruf der mit der gesetzlichen Zeit synchronisierten Systemzeit des SMGW,
- Auslösen von Neustart und Selbsttest des SMGW,
- Auslösen der Nutzerdatenbereinigung des SMGW,
- Auslesen von Kommunikationsprofilen,
- Auslesen der Konfigurationsparameter und des Zustandes des Netzwerkschnittstellen des SMGW,
- Änderung der Kommunikationsparameter der WAN-Schnittstelle und zum GWA-Kommunikationssystem zur Wiederherstellung der Kommunikation mit dem GWA.

2.3.5 Weitere Funktionen des SMGW

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

Nutzerverwaltung/Mandantenfähigkeit

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

Kryptographische Funktionen

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

Das Sicherheitsmodul erfüllt die Anforderungen aus [TR-03109-2]. [PP-0073] beschreibt, welche kryptografischen Funktionen vom Sicherheitsmodul übernehmen werden.

Protokollierung

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

- **System-Log**

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

- **Anschlussnutzer-Log**

  Alle Transaktionen des SMGW, z.B. das Versenden von Messwerten, und die den Anschlussnutzer betreffenden Aktivitäten des GWA werden in einem Anschlussnutzer-Log mit begrenzten Vorhaltefristen festgehalten. Ein authentifizierter und autorisierter Anschlussnutzer kann die ihn betreffenden Informationen vom SMGW über die HAN-Schnittstelle für Anzeigeeinheiten abrufen und somit nachverfolgen, wer wann welche Daten erhalten hat, oder ob benutzerbezogene Daten (z.B. Profile) geändert bzw. hinzugefügt oder entfernt wurden.

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

- **Eichtechnisches Logbuch**

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

Zu protokollierende Ereignisse werden aus Anforderungen referenziert und sind normativ umzusetzen. ▸Tabelle A.1 enthält die Übersicht der zu protokollierenden Ereignisse.

2.4 Interoperabilitätsmodell

2.4.1 Einleitung

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

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

2.4.2 Begriffsdefinitionen

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

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

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

2.4.3 Interoperabilitäts-Modell der Technischen Richtlinie

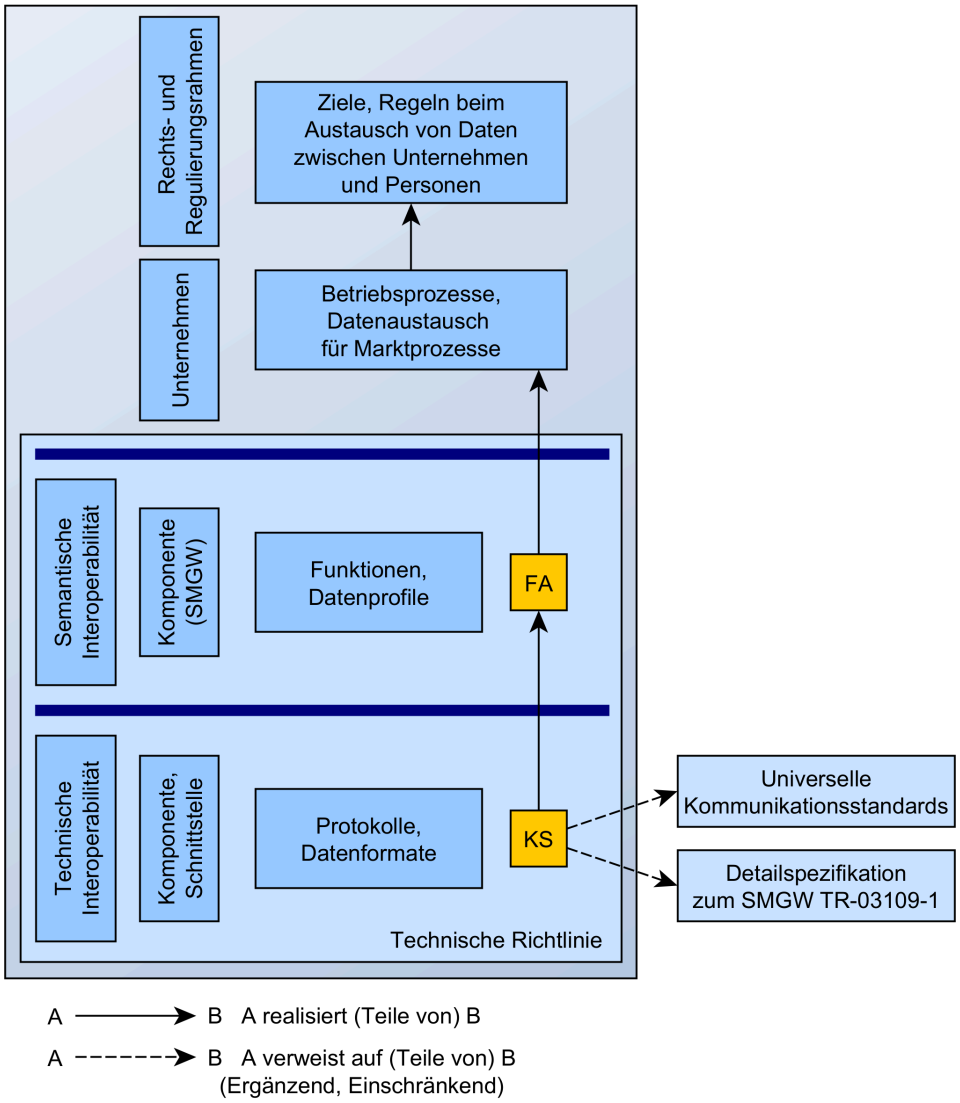


Abbildung 2.2. Interoperabilitäts-Modell der Technischen Richtlinie

Das Interoperabilitäts-Modell (▸Abbildung 2.2) zeigt die Hierarchie der Anforderungen: Oben steht der Rechts- und Regulierungsrahmen, der die Ziele und Regeln beim Austausch von Daten zwischen Unternehmen und Personen beschreibt. Diese werden durch die Unternehmen mit einheitlichen Datenaustausch-Prozessen realisiert. Darunter stellt die Grafik den Beitrag dieser Technischen Richtlinie zur Umsetzung der Semantischen und Technischen Anforderungen an Komponenten dar: fachliche Anwendungsfälle (FA) beschreiben die semantische Interoperabilität, d.h. Funktionalität und Datenprofile und realisieren damit einen Teil der Unternehmensprozesse, Kommunikationsszenarien (KS) beschreiben die technische Interoperabilität, d.h. Protokolle und Datenformate, die Teile der FA an den Schnittstellen realisieren. Sofern externe bzw. universelle Kommunikationsstandards zur Verbesserung der Interoperabilität konkretisiert werden müssen, wird dies durch Verweise auf Kapitel der Detailspezifikation zur TR-03109-1 realisiert.

In ▸Kapitel 3 werden Anforderungen auf semantischer Ebene betrachtet und fachliche Anwendungsfälle formuliert. Dabei umfasst ein FA eine Funktionalität, die aufgrund interner oder externer *Ereignisse* von einem SMGW abgearbeitet wird. Diese Funktionalität wird im FA semantisch beschrieben, Kommunikationsprotokoll- und syntaktische Details werden an dieser Stelle abstrahiert. Anforderungen an die Protokolle zur Kommunikation werden in *Kommunikationsszenarien* (KS) zusammengefasst.

In ▸Kapitel 4 werden die Anforderungen an die KS beschrieben (technische und syntaktische Ebene). Dabei wird die technische Interoperabilität durch Vorgaben an die Protokolle und Datenformate (Transfersyntax) erreicht.

Detailspezifikationen (DS) (siehe [DS]) konkretisieren universelle Kommunikationsstandards zur weiteren Verbesserung der technischen Interoperabilität von Protokollen und Datenstrukturen der KS.

In ▸Abbildung 2.2 wird dieser Zusammenhang zwischen FA, KS und DS abgebildet: FA enthalten Anforderungen an die Funktionalität und Verweise auf KS, die die Anforderungen an die Protokollstandards für die Kommunikation mit Kommunikationspartnern des SMGW konkretisieren.

2.5 Fachliche Anwendungsfälle und FA-Kategorien

2.5.1 Beschreibung der Struktur

Die grundlegende Funktionalität des SMGW wird im Rahmen dieser Technischen Richtlinie in Form von Fachlichen Anwendungsfällen (FA) in ▸Kapitel 3 beschrieben. Ein FA definiert eine thematisch abgegrenzte Funktionalität des SMGW und bündelt zu deren Erfüllung notwendige Anforderungen. Normativ zu erfüllende Anforderungen in diesem Kapitel sind durch Anforderungs-IDs beginnend mit "REQ" zu erkennen. Weitere Inhalte haben informativen Charakter. Zu beachten ist, dass die Umsetzung einiger Anforderungen erst zu einem späteren Zeitpunkt verpflichtend wird (siehe ▸Abschnitt 1.6).

Wird die Realisierung eines FA in der FA-Kategorie mit **SOLL** gefordert und ist dieser gemäß ICS nicht implementiert, dann werden die Anforderungen zur Interoperabilität des FA nicht geprüft. Dies gilt (transitiv) für die daraus referenzierten Anforderungen in Kommunikationsszenarien und den daraus referenzierten Kapiteln der Detailspezifikation.

FA-Kategorien sind Zusammenfassungen mehrerer FA, die fachlich zusammengehören und einem auslösenden Akteur, in der Regel an einer Kommunikationsschnittstelle, zugeordnet sind. Die Verpflichtung zur Umsetzung eines FA kann - für verschiedene Akteure - aus mehr als einer FA-Kategorie gefordert sein.

Der Aufbau einer FA-Kategorie folgt der folgenden Struktur:

Überschrift — Die Überschrift eines Abschnitts, in dem eine FA-Kategorie beschrieben wird, enthält einen kurzen Namen zur Erläuterung des darin beschriebenen Themenbereichs gefolgt von einer ID.

Übersicht — Die Übersicht beinhaltet eine Beschreibung des in der FA-Kategorie behandelten Themas und kann weitere Details, wie Zusammenhänge zwischen FA beschreiben.

Übersicht der FA — Innerhalb dieses Abschnitts findet sich eine Übersichtstabelle, die alle in der FA-Kategorie relevanten Aufgaben und die dazu notwendigen FA beinhaltet. Die Tabelle enthält auch eine Aussage über die Verpflichtung zur Umsetzung des jeweiligen FA und des Akteurs, für den der FA umgesetzt wird, sofern ein Akteur benannt werden kann. Die verwendeten Kommunikationsszenarien sind im FA selbst definiert.

Vereinzelt werden für Aufgaben einer FA-Kategorie auch FA aus anderen FA-Kategorien referenziert.

Datenstrukturen — Die Bedeutungen der Datenfelder und ihrer Wertebereiche von Datenstrukturen, die innerhalb der FA-Kategorie relevant sind, sind in ▸Abschnitt 2.6 beschrieben.

Weitere Anforderungen — Unterabschnitte beschreiben weitere Anforderungen der FA-Kategorie, die neben den FA gelten.

In den weiteren Abschnitten werden die jeweiligen FA der FA-Kategorie beschrieben. Die folgende Liste beschreibt die Gliederung der FA-Abschnitte innerhalb einer FA-Kategorie.

Überschrift — Die Überschrift eines Abschnitts, in dem der FA beschrieben wird, ist eine eindeutige ID, um den FA leicht identifizieren und referenzieren zu können. Die ID folgt dabei einer Namenskonvention, die in der Detailspezifikation "RESTful Webservice" erläutert ist.

Beschreibung — Die Beschreibung gibt einen groben Überblick über die Aufgabe und den Sinn des FA.

Auslöser — Dieser Abschnitt beschreibt die verschiedenen Auslöser, die das Ausführen des FA zur Folge haben.

Ein Auslöser besteht immer aus einem eintretenden Ereignis. Dies kann eine Anfrage über ein Kommunikationsszenario oder ein internes Ereignis (z.B. Erreichung bestimmter Zeit) sein. Sofern vorhanden, werden relevante Kommunikationsszenarien ebenfalls benannt. Ist zum Kommunikationsszenario eine Rolle benannt, dann gilt der Auslöser nur für Akteure der genannten Rolle. Ist keine Rolle benannt, dann gilt der Auslöser für alle Rollen, die das genannte Kommunikationsszenario nutzen können.

Bei den Auslösern und der daraufhin folgenden Ausführung der Schritte des FA (siehe "Anforderungen") wird im Falle von Anfragen durch einen Akteur von den nachfolgenden Annahmen ausgegangen. Da es sich um Annahmen handelt, finden keine Prüfung durch Anforderungen des FA statt. Anforderungen an diese Prüfungen und daraus resultierende Aktionen können durch andere Teile der TR bestehen.

- Bei Anfragen zum Zugriff auf identifizierte Datenstrukturen ist die angefragte Datenstruktur auf dem SMGW vorhanden. Zugriffe auf nicht vorhandene identifizierte Datenstrukturen werden im Rahmen des jeweiligen Kommunikationsszenarios aus Kapitel ▸4 behandelt und beantwortet.
- Beim Einbringen von identifizierten Datenstrukturen in das SMGW ist keine Datenstruktur auf dem SMGW vorhanden, die dieselbe Identifikation besitzt. Konflikte beim Einbringen werden im Rahmen des jeweiligen Kommunikationsszenarios aus Kapitel ▸4 behandelt und beantwortet.
- Einzubringende Datenstrukturen sind syntaktisch korrekt und vollständig bezogen auf ihre Definition. Fehlende optionale Datenfelder sind mit den beschriebenen Standardwerten befüllt. Ungültige Datenstrukturen werden im Rahmen des jeweiligen Kommunikationsszenarios aus Kapitel ▸4 behandelt. Semantische Prüfungen - wie z.B. Plausibilisierung von Datenfelder abhängig vom Kontext - wird im Rahmen des jeweiligen FA beschrieben. Siehe dazu auch ▸Anhang D GWA8.
- Der Akteur ist in seiner Rolle zum Zugriff auf die Datenstruktur beziehungsweise zum Auslösen des angefragten FA berechtigt. Die Berechtigung zur Kommunikation wird über die Abläufe des Kommunikationsszenarios aus Kapitel ▸4 festgelegt. Die Berechtigung zum Zugriff wird für die Rolle über die Anforderungen in der Übersichtstabelle der jeweiligen FA-Kategorie, detaillierter für die HAN-Schnittstelle in ▸Anhang C und allgemein über die Anforderungen des [PP-0073] festgelegt.

Anforderungen

Dieser Abschnitt beinhaltet die Anforderungen, die im Rahmen dieses FA gelten, sowie weitere Informationen. Es gilt dabei die folgende Reihenfolge, wobei nicht jedes Element in jedem FA zu finden ist:

- Eine unnummerierte Liste von Anforderungen. Sofern Anforderungen Prüfschritte beschreiben, stellt die Reihenfolge eine Empfehlung aber keine Vorgabe dar.
- Unter der Überschrift "ICS" werden ebendiese benannt. ICS definieren, welche zusätzlichen Informationen der Hersteller über die Implementierung des SMGW deklarieren muss.

Enthält eine Anforderung mehrere Sätze, gilt das Modalverb des ersten Satzes auch für die folgenden Sätze der Anforderung.

Beginnt eine Anforderung mit einem Ausdruck in Klammern, so ist die Anforderung abhängig von der Bedingung im Ausdruck.

Endet die Anforderung mit einem Verweis auf ein oder mehrere Ereignisse, so sind diese gemäß Anhang ▸Anhang A zu protokollieren und ggf. der GWA zu benachrichtigen.

Implementierungshinweise In diesem Abschnitt werden zusätzliche Hinweise gegeben, die für die Implementierung des SMGW relevant sind. Diese Informationen stellen keine normativ umzusetzenden Anforderungen dar. Es ist jedoch dringend empfohlen, dass der Hersteller des SMGW sie bei der Implementierung berücksichtigt.

2.5.2 Identifikation der vom SMGW bereitgestellten Messgrößen

Dieser Abschnitt beschreibt die Identifikation der im Rahmen der Mindestanforderungen vom SMGW bereitgestellten Messgrößen mittels OBIS-IDs gemäß [EN62056-6-1] für elektrische Energie und [EN13757-1] für Gas und andere Sparten. Das SMGW stellt die Messwerte am HAN (siehe ▸FAKAT.ConServices) und WAN (siehe ▸FAKAT.ValTransmission) bereit.

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

Zur Abrechnung und Bilanzierung elektrische Energie wird die Messgröße Energie verwendet. Die Bezeichnung "Arbeit" wird in diesem Kontext Synonym zu Energie verwendet. Verkehrsgebräuchliche Einheit[2] für die Abrechnung elektrischer Wirkenergie ist kWh. Blindenergie wird mit der Einheit kvarh bereitgestellt.

Zur Abrechnung und Bilanzierung thermischer Energie aus Gas wird zunächst das Betriebs- oder Normvolumen des Energieträgers (Erd-)Gas (und ggf. die Zustandsgrößen Druck, Temperatur) in der Messeinrichtung gemessen. Die Umrechnung des vom SMGW bereitgestellten Gas-Volumens in thermische Energie zur Abrechnung erfolgt beim EMT (in der Regel Netzbetreiber für Gas). Verkehrsgebräuchliche Einheit für das Volumen ist m^3.

Zur Abrechnung thermischer Energie, die durch Wasser übertragen wird, wird Volumen/Durchflussmenge und Temperaturdifferenz in einer Messeinrichtung gemessen. Die Umrechnung in thermische Energie zur Abrechnung erfolgt in der Messeinrichtung. Verkehrsgebräuchliche Einheit für thermische Energie ist kWh. Zählerstände entzogener Energie ("Kälte") und gelieferter Energie ("Wärme") werden über unterschiedliche OBIS-IDs identifiziert.

Zur Abrechnung von Leitungswasser wird das Volumen in einer Messeinrichtung gemessen und zur Abrechnung verwendet. Zählerstände für nicht erwärmtes Leitungswasser ("Kaltwasser") und erwärmtes Trinkwasser ("Warmwasser") werden über unterschiedliche OBIS-IDs identifiziert.

Die mit Heizkostenverteilern (Heat Cost Allocators) am Heizkörper erfassten Einheiten werden beim EMT (in der Regel Submetering-Dienstleister) in Verbrauchs- und Abrechnungsinformationen umgerechnet, da dazu weitere Informationen benötigt werden, die nicht im SMGW vorliegen.

Das SMGW stellt Zählerstände bzw. Zählerstandsgänge zur Abrechnung, Bilanzierung und zur Information bereit. Zählerstände sind grundsätzlich positive Werte. Momentanwerte können auch negativ sein.

OBIS-IDs werden in diesem Dokument zur besseren Lesbarkeit im Format A-B:C.D.E[*F] notiert. A-F werden als dezimale Ganzzahlen ohne führende "0" notiert. Die Bedeutung der Wertegruppen A-F bei der Identifikation der Messwerte, für die im SMGW verarbeiteten Sparten wird in der folgenden Tabelle erläutert. Die Definition der Wertegruppen erfolgt in [EN62056-6-1] und [EN13757-1][3]. Zählerstände vorheriger Abrechnungsperioden (Vorwerte) werden nicht über die Wertegruppe F, sondern über den Zeitstempel zum Messwert identifiziert. Zur besseren Lesbarkeit wird im Folgenden die Identifikation "*255" der Wertegruppe weggelassen.

Welche OBIS-IDs bereitgestellt werden, wird über Auswertungsprofile (TAF) und die Fähigkeiten der verbundenen Messeinrichtungen bestimmt.

▸Tabelle 2.1 enthält eine Übersicht der Systematik der OBIS-IDs der in dieser Technischen Richtlinie verwendeten Sparten, abgeleitet aus [EN62056-6-1] und [EN13757-1].

▸Tabelle 2.2 und ▸Tabelle 2.3 beschreiben exemplarisch die Teilmenge aus [EN62056-6-1] und [EN13757-1], die für die Mindestinteroperabilität der Messwertverarbeitung nach dieser Technischen Richtlinie an den Schnittstellen verwendet wird.

---

[2] Verkürzt wird "Einheit" verwendet, wenn das Einheitenzeichen mit optionalem Einheitenvorsatzzeichen bzw. Präfix gemeint ist.

[3] Die Identifikation von Messeinrichtung, Status und Registrierzeitpunkt werden über Datenfeldbezeichner in Datenstrukturen gemäß Spezifikation der jeweiligen Schnittstelle identifiziert.

Wertegruppe	Bedeutung Sparte 1	Bedeutung Sparte 7	Bedeutung Sparte 5/6 Thermische Energie	Bedeutung Sparte 8/9 Wasser
A (Sparte)	1: Elektrische Energie	7: (Erd-)Gas	4: Heizkosten-Einheiten 5: Kälte 6: Wärme	8: Kaltwasser 9: Warmwasser
B (Kanal)	0			
C (Messgröße)[4][5]	1: Wirkenergie (Bezugsrichtung) (für D=8) 2: Wirkenergie (Lieferrichtung) (für D=8) 3: Blindenergie (Bezugsrichtung) (für D=8) 4: Blindenergie (Lieferrichtung) (für D=8) 5..8: Blindenergie (Quadrant I, II, III, IV) (für D=8) 14: Frequenz 16: Wirkleistung (Summe phasensaldierend über Leiter L1, L2, L3) (für D=7) 31,51,71: Strom (Leiter L1, L2, L3) (für D=7) 32,52,72: Spannung (Leiter L1-N, L2-N, L3-N) (für D=7) 36,56,76: Wirkleistung (Leiter L1-N, L2-N, L3-N) (für D=7) 81: Phasenwinkel (für D=7) Registrierende Messeinrichtungen für elektrische Energie können weitere Werte dieser Wertegruppe gemäß [EN62056-6-1] übermitteln.	3: Volumen (Bezugsrichtung bzw. Richtung nicht im SMGW festgelegt) 6: Volumen (Lieferrichtung) 41: Temperatur, absolut 42: Druck, absolut Registrierende Gasmesseinrichtungen und Mengenumwerter können weitere Werte dieser Wertegruppe gemäß [EN13757-1] übermitteln.	1: Energie 2: Volumen 8: Leistung 9: Durchfluss 10: Vorlauftemperatur 11: Rücklauftemperatur	1: Volumen 2: Durchfluss

[4] Eine positive Bezugsrichtung kennzeichnet den Energie-/Volumenfluss in Richtung Netznutzer.

[5] Eine positive Lieferrichtung kennzeichnet den Energie-/Volumenfluss in Richtung des Netzes.

Wertegruppe	Bedeutung Sparte 1	Bedeutung Sparte 7	Bedeutung Sparte 5/6 Thermische Energie	Bedeutung Sparte 8/9 Wasser
D (Messart)	6: Maximalwert im Berichtszeitraum 7: Momentanwert[6] 8: Zeitintegral 1 (Integration der Messgröße seit Herstellung des Zählers)[7] 29: Zeitintegral 5 (Integration der Messgröße seit Beginn der Messperiode (letzter Registrierzeitpunkt), äquidistante Dauer) Weitere Messarten (Maximumwerte, Vorschübe/Mengen) werden im Rahmen der Mindestinteroperabilität nicht verwendet. Registrierende Messeinrichtungen für elektrische Energie können weitere Werte dieser Wertegruppe gemäß [EN62056-6-1] übermitteln.	Für C=3, 6: 0: Zählerstand bei *Betriebsbedingungen* 1: Zählerstand, temperaturkorrigiert 2: Zählerstand bei *Normbedingungen* Registrierende Gasmesseinrichtungen und Mengenumwerter können weitere Werte dieser Wertegruppe gemäß [EN13757-1] übermitteln.	0: Aktueller Wert 2: Wert am Stichtag	
E	Tarifstufe: 0: Keine Tarifstufe (Total) Für C gleich 1-8 ist E=1..62: Menge in Tarifstufe 1..62 Für C gleich 1-8: E=63: Menge, die keiner Tarifstufe zugeordnet werden kann Für C gleich 81: Leiter zwischen denen der Phasenwinkel gemessen wird 1: U-L2 zu U-L1 2: U-L3 zu U-L1 4: I-L1 zu U-L1 15: I-L2 zu U-L2 26: I-L3 zu U-L3	Mittelungszeitraum 0	0	
F (Vorwert)	255: Aktueller Wert gemäß Zeitstempel			

Tabelle 2.1 Bedeutung der OBIS-Wertegruppen

OBIS-ID	Bedeutung	Einheit
Elektrische Energie		
1-B:1.8.0	Elektrische Wirkenergie (A+, Bezugsrichtung) Zählerstand (total)	kWh
1-B:2.8.0	Elektrische Wirkenergie (A-, Lieferrichtung) Zählerstand (total)	kWh
1-B:1.8.E	Elektrische Wirkenergie Bezug, tarifierter Zählerstand der Tarifstufe (E=1..62,63)	kWh
1-B:2.8.E	Elektrische Wirkenergie Lieferung, tarifierter Zählerstand der Tarifstufe (E=1..62,63)	kWh

[6] Momentanwerte sind eine Momentaufnahme zum Messzeitpunkt, haben keinen Bezug zu Registrierperioden und können sich kurzfristig ändern.

[7] Zur Verkürzung der Schreibweise wird statt "Zeitintegral der Leistung über alle Außenleiter (Phasen)" "Zählerstand elektrische Energie" verwendet.

OBIS-ID	Bedeutung	Einheit
1-B:3.8.0	Elektrische Blindenergie (R+, Bezugsrichtung) Zählerstand (total)	kvarh
1-B:4.8.0	Elektrische Blindenergie (R-, Lieferrichtung) Zählerstand (total)	kvarh
1-B:3.8.E	Elektrische Blindenergie Bezug, tarifierter Zählerstand der Tarifstufe (E=1..62,63)	kvarh
1-B:4.8.E	Elektrische Blindenergie Lieferung, tarifierter Zählerstand der Tarifstufe (E=1..62,63)	kvarh
1-B:5.8.0	Elektrische Blindenergie (Quadrant I)	kvarh
1-B:6.8.0	Elektrische Blindenergie (Quadrant II)	kvarh
1-B:7.8.0	Elektrische Blindenergie (Quadrant III)	kvarh
1-B:8.8.0	Elektrische Blindenergie (Quadrant IV)	kvarh
1-B:1.29.0	Mittlere elektrische Wirkleistung (Bezugsrichtung) Mittlere Leistung pro Registrierperiode (Lastgang)	W
1-B:2.29.0	Mittlere elektrische Wirkleistung (Lieferrichtung) Mittlere Leistung pro Registrierperiode (Lastgang)	W
Gas		
7-B:3.0.0	Gasvolumen (Zählerstand) bei *Betriebsbedingungen*[8]	m³
7-B:3.1.0	Gasvolumen (Zählerstand) bei *Betriebsbedingungen* (Temperaturkompensiert)	m³
7-B:3.2.0	Gasvolumen (Zählerstand) bei *Normbedingungen*	m³
7-B:6.0.0	Gasvolumen (Zählerstand) Einspeisung bei *Betriebsbedingungen*	m³
7-B:41.0.0	Temperatur nur zusammen mit 7-B:3.2.0 übermittelt	°C/K
7-B:41.2.0	Temperatur nur zusammen mit 7-B:3.2.0 übermittelt	°C/K
7-B:42.2.0	Druck (absolut) nur zusammen mit 7-B:3.2.0 übermittelt	bar
Thermische Energie		
4-B:1.0.0	Heizkosten Einheiten zur Verbrauchsaufteilung (Wärme)	-
5-B:1.0.0	Thermische Energie (Zählerstand), Kälte. Im Kontext dieser TR "Verbrauch"	kWh
6-B:1.0.0	Thermische Energie (Zählerstand) Wärme. Im Kontext dieser TR "Verbrauch"	kWh
Wasser		
8-B:1.0.0	Kumuliertes Wasservolumen (Zählerstand) Kaltwasser. Im Kontext dieser TR "Verbrauch"	m³
9-B:1.0.0	Kumuliertes Wasservolumen (Zählerstand) Warmwasser. Im Kontext dieser TR "Verbrauch"	m³

Tabelle 2.2 OBIS-IDs zur Abrechnung und Information

OBIS-ID	Bedeutung	Einheit
Elektrische Energie		
1-0:c.7.0	Momentanwerte zur elektrischen Energiemessung gemäß [EN62056-6-1]. Das Vorhandensein hängt von den Fähigkeiten der Messeinrichtung und der Konfiguration im Auswertungsprofil ab.	Je nach Messgröße: A/V/W/Hz/%
1-0:c.8.0	Aktuelle Zählerstände. Das Vorhandensein hängt von den Fähigkeiten der Messeinrichtung und der Konfiguration im Auswertungsprofil ab.	Je nach Messgröße: kvarh/kWh
1-0:16.7.0	Momentane Wirkleistung (P) über alle Phasen gebildet in der Messeinrichtung. Positive Werte identifizieren bezogene Leistung (Ausnahme: Bei Einrichtungs-Einspeisezählern identifiziert ein positiver Wert die eingespeiste Momentanleistung.) Bei Zweirichtungszählern identifiziert ein negativer Wert die eingespeiste Momentanleistung.	W
1-0:32.7.0	Momentane Spannung (U) Außenleiter L1. Gemessen in der Messeinrichtung.	V
1-0:52.7.0	Momentane Spannung (U) Außenleiter L2. Gemessen in der Messeinrichtung.	V

[8] Verwendet bei Gas-SLP Abrechnung ("Haushaltskunden")

OBIS-ID	Bedeutung	Einheit
1-0:72.7.0	Momentane Spannung (U) Außenleiter L3. Gemessen in der Messeinrichtung.	V
1-0:31.7.0	Momentaner Strom (I) Außenleiter L1. Gemessen in der Messeinrichtung.	A
1-0:51.7.0	Momentaner Strom (I) Außenleiter L2. Gemessen in der Messeinrichtung.	A
1-0:71.7.0	Momentaner Strom (I) Außenleiter L3. Gemessen in der Messeinrichtung.	A
1-0:36.7.0	Momentane Wirkleistung (P) Außenleiter L1. Gemessen in der Messeinrichtung.	W
1-0:56.7.0	Momentane Wirkleistung (P) Außenleiter L2. Gemessen in der Messeinrichtung.	W
1-0:76.7.0	Momentane Wirkleistung (P) Außenleiter L3. Gemessen in der Messeinrichtung.	W
Gas		
7-0:3.D.0	Momentane Gas-Zählerstände. Das Vorhandensein hängt von den Fähigkeiten der Messeinrichtung und der Konfiguration im Auswertungsprofil ab.	m³
7-0:43.D.0	Momentane Durchflussmenge (m³/h). Das Vorhandensein hängt von den Fähigkeiten der Messeinrichtung und der Konfiguration im Auswertungsprofil ab.	m³/h
Thermische Energie		
5-0:8.0.0	Momentanleistung (Kältezähler). Das Vorhandensein hängt von den Fähigkeiten der Messeinrichtung und der Konfiguration im Auswertungsprofil ab.	W
5-0:9.0.0	Momentane Durchflussmenge (Kältezähler). Das Vorhandensein hängt von den Fähigkeiten der Messeinrichtung und der Konfiguration im Auswertungsprofil ab.	m³/h
5-0:10.0.0	Momentane Vorlauftemperatur (Kältezähler). Das Vorhandensein hängt von den Fähigkeiten der Messeinrichtung und der Konfiguration im Auswertungsprofil ab.	°C
5-0:11.0.0	Momentane Rücklauftemperatur (Kältezähler). Das Vorhandensein hängt von den Fähigkeiten der Messeinrichtung und der Konfiguration im Auswertungsprofil ab.	°C
6-0:8.0.0	Momentanleistung (Wärmezähler). Das Vorhandensein hängt von den Fähigkeiten der Messeinrichtung und der Konfiguration im Auswertungsprofil ab.	W
6-0:9.0.0	Momentane Durchflussmenge (Wärmezähler). Das Vorhandensein hängt von den Fähigkeiten der Messeinrichtung und der Konfiguration im Auswertungsprofil ab.	m³/h
6-0:10.0.0	Momentane Vorlauftemperatur (Wärmezähler). Das Vorhandensein hängt von den Fähigkeiten der Messeinrichtung und der Konfiguration im Auswertungsprofil ab.	°C
6-0:11.0.0	Momentane Rücklauftemperatur (Wärmezähler). Das Vorhandensein hängt von den Fähigkeiten der Messeinrichtung und der Konfiguration im Auswertungsprofil ab.	°C
Wasser		
8-0:2.0.0	Momentane Durchflussmenge (Kaltwasserzähler). Das Vorhandensein hängt von den Fähigkeiten der Messeinrichtung und der Konfiguration im Auswertungsprofil ab.	m³/h
9-0:2.0.0	Momentane Durchflussmenge (Warmwasserzähler). Das Vorhandensein hängt von den Fähigkeiten der Messeinrichtung und der Konfiguration im Auswertungsprofil ab.	m³/h

Tabelle 2.3 OBIS-IDs zur Information

2.6 Datenstrukturen und Profile

2.6.1 Übersicht

Dieser Abschnitt listet die in dieser Technischen Richtlinie verwendeten Datenstrukturen in alphabetischer Reihenfolge auf.

Ein "Ja" in der Spalte "Vorkonfiguriert" kennzeichnet, dass ein Profil nicht über "Create" angelegt, aber über "Update" aktualisiert werden kann, da bereits ein initiales Profil mit Default-Parametern vom Hersteller angelegt wurde. Ein "n/a" kennzeichnet, dass die Vorkonfiguration auf dieses Profil nicht anwendbar ist (z.B., weil es sich um Statusprofile handelt).

Ein "Ja" in der Spalte "Persistent" kennzeichnet, dass ein Profil über einen Neustart des SMGW hinaus gespeichert werden muss.

Name	Referenz	Vorkonfiguriert	Persistent	Beschreibung
Profile				
Auswertungsprofil	▶Abschnitt 3.22.6	Nein	Ja	Konfigurationsparameter für das Auswertungsprofil eines TAF zur Messwertverarbeitung
Benachrichtigungsprofil	▶Abschnitt 3.22.9	Ja	Ja	Konfigurationsparameter, die bestimmen, welche Ereignisse den GWA benachrichtigen
Firmware-Update Profil (SMGW)	▶Abschnitt 3.22.18	Ja	Ja	Konfigurationsparameter zum Download und Installation von Firmware
HAN-Schnittstellenkonfigurationsprofil	▶Abschnitt 3.22.21	Ja	Ja	Konfigurationsparameter für die physische(n) HAN-Schnittstelle(n)
HAN-Kommunikationsprofil	▶Abschnitt 3.22.22	Nein	Ja	Konfigurationsparameter für die Kommunikation mit Anschlussnutzern und Servicetechnikern
LMN-Schnittstellenprofil	▶Abschnitt 3.22.24	Ja	Ja	Konfigurationsparameter für die physische(n) LMN-Schnittstellen(n)
LMN-Kommunikationsprofil	▶Abschnitt 3.22.25	Nein	Ja	Konfigurationsparameter für die Kommunikation mit Messeinrichtungen
Netzwerkdiagnose-Konfigurationsprofil	▶Abschnitt 3.22.30	Nein	Ja	Konfigurationsparameter für die Netzwerkdiagnose
Proxy-Kommunikationsprofil	▶Abschnitt 3.22.37	Nein	Ja	Konfigurationsparameter für die TLS-Proxy Kommunikation
WAN-Kommunikationsprofil (EMT)	▶Abschnitt 3.22.46	Nein	Ja	Konfigurationsparameter zur Kommunikation mit dem EMT im WAN
WAN-Kommunikationsprofil (GWA)	▶Abschnitt 3.22.46	Ja	Ja	Konfigurationsparameter zur Kommunikation mit dem GWA im WAN
WAN-Schnittstellenkonfigurationsprofil	▶Abschnitt 3.22.45	Ja	Ja	Konfigurationsparameter für die physische(n) WAN-Schnittstelle(n)
Datenstrukturen der Ausgabe				
Abgeleiteter Wert und abgeleitete Werteliste (AWL)	▶Abschnitt 3.22.4	Nein	Ja	Vom SMGW bereitgestellte Abgeleitete Wertliste
CLS-Statusliste	▶Abschnitt 3.22.12	n/a	Nein	Liste der an das SMGW kommunikativ angebundenen CLS
Device-Info (SMGW)	▶Abschnitt 3.22.15	Ja	Ja	Geräteinformationen (z.B. Hardware und Firmware, Typ und Identifikation des SMGW)
Device-Status	▶Abschnitt 3.22.16	n/a	Nein	Gerätestatus des SMGW oder einer Messeinrichtung
Export-Datenstruktur	▶Abschnitt 3.22.17	Nein	Nein	Struktur, um Messwerte und andere Daten signiert bereitzustellen
Eingangsmesswerte	▶Abschnitt 3.22.5	Nein	Nein	Struktur und Bedeutung der von einer Messeinrichtung an das SMGW übermittelten Daten
GWA-Schlüsselreferenzen	▶Abschnitt 3.22.20	Ja	Nein	Struktur zur Bereitstellung der Schlüsselreferenzen für den GWA aus dem Sicherheitsmodul des SMGW für den GWA. Es sind zwei Schlüsselbänke angelegt.
Logbuch und Ereignisse	▶Abschnitt 3.22.26	n/a	Ja	Struktur zur Bereitstellung von Logbucheinträgen

Name	Referenz	Vorkonfiguriert	Persistent	Beschreibung
Netzwerkdiagnose-Status	▸Abschnitt 3.22.32	n/a	Nein	Struktur und Bedeutung der Netzwerkdiagnosedaten
Nichtvalidierte Messwerte und -Messwertliste (NWL)	▸Abschnitt 3.22.33	Nein	Nein	Vom SMGW bereitgestellte Nichtvalidierte Messwertliste
Proxy-Statusprofil	▸Abschnitt 3.22.38	n/a	Nein	Statusinformationen eines Proxy-Kommunikationskanals
Registrierter Wert und Registrierte Werteliste (RWL)	▸Abschnitt 3.22.35	Nein	Ja	Vom SMGW bereitgestellte Registrierte Wertliste
Zustand des Sicherheitsmoduls	▸Abschnitt 3.22.40	n/a	Nein	Zustandsinformationen des Sicherheitsmoduls
SMGW-Schlüsselreferenzen	▸Abschnitt 3.22.23	Ja	Ja	Struktur zur Bereitstellung der Schlüsselreferenzen für Schlüsselobjekte. Eine Schlüsselbank ist im Sicherheitsmodul vorkonfiguriert.
SMGW-Zertifikatssatz	▸Abschnitt 3.22.42	Ja	Ja	Zertifikatssatzes der SM-PKI-Zertifikate für das SMGW
Tageswertliste (TWL) und Tageswerte	▸Abschnitt 3.22.43	Nein	Ja	Täglich erfasste Zählerstände der Messeinrichtung
Tarifzustand	▸Abschnitt 3.22.44	n/a	Nein	Aktueller Zustand des Verarbeitungsprogrammes für einen Tarif mit abgeleiteten Werten
Zählerstatusliste	▸Abschnitt 3.22.29	n/a	Nein	Liste der an das SMGW kommunikativ angebundenen Messeinrichtungen
Zeitsynchronisationsstatus	▸Abschnitt 3.22.47	Nein	Nein	Statusinformationen der Uhr und der Zeitsynchronisation
Zertifikat	▸Abschnitt 3.22.48	Ja (*)	Ja	Struktur zur Bereitstellung eines X.509 Zertifikates. Initiale GWA-, RootCA, SubCA- und SMGW-Zertifikate sind vorkonfiguriert.
Zertifikat und Schlüssel	▸Abschnitt 3.22.10	Nein	Nein	Vom SMGW erzeugtes Zertifikat und privater Schlüssel als Ergebnis des Zertifikatserstellungsdienstes
Parameter für FA-Auslösung				
AuthChallenge	▸Abschnitt 3.22.7	n/a	Nein	Aufrufparameter mit Zufallszahl (Challenge)
AuthResponse	▸Abschnitt 3.22.8	n/a	Nein	Aufrufparameter zur Authentifizierung mit signiertem Token
CgrParameters	▸Abschnitt 3.22.11	n/a	Nein	Aufrufparameter zur Schlüssel- und Zertifikatserzeugung
CsrParameters	▸Abschnitt 3.22.14	n/a	Nein	Aufrufparameter zur Erzeugung eines Certificate Signing Requests
GWA-Wechselparameter	▸Abschnitt 3.22.19	n/a	Nein	Aufrufparameter zur Einleitung des GWA-Wechsels
LogTrunc Parameter	▸Abschnitt 3.22.27	n/a	Nein	Aufrufparameter zur Kürzung von Logbüchern
OnDemand Parameter	▸Abschnitt 3.22.34	n/a	Nein	Aufrufparameter zum Auslösen der Bedarfsauslesung
Passwort-Update Parameter	▸Abschnitt 3.22.36	n/a	Nein	Aufrufparameter für die Passwort-Aktualisierung

Name	Referenz	Vorkonfiguriert	Persistent	Beschreibung
RootCA-Zertifikatssatz	▸Abschnitt 3.22.39	n/a	Ja	Aufrufparameter zum Import eines RootCA-Zertifikates mit Link-Zertifikat
Selbsttest-Parameter	▸Abschnitt 3.22.41	n/a	Nein	Aufrufparameter für Selbsttests
Eingebettete Datenstrukturen				
Kombiniertes Statuswort	▸Abschnitt 3.22.13	n/a	Nein	Kombination des SMGW- und des Zählerstatuswortes
Messgerätestatus	▸Abschnitt 3.22.28	n/a	Nein	Informationen zum Status einer Messeinrichtung
Netzwerkdiagnose-Attribute	▸Abschnitt 3.22.31	n/a	Nein	Zulässige Attribute für die Netzwerkdiagnosedaten

Tabelle 2.4 Liste der Datenstrukturen und Profile

3 Funktionale Anforderungen an das SMGW

3.1 Einleitung

In diesem Kapitel werden Anforderungen an die Funktionalität und Interoperabilität des SMGW gestellt, beispielsweise an die Messwertverarbeitung und die an den Schnittstellen des SMGW für die unterschiedlichen Rollen bereitzustellenden Dienste.

Die Beschreibung der funktionalen Anforderungen erfolgt durch fachliche Anwendungsfälle, die das SMGW umsetzt.

▸Abbildung 3.1 zeigt eine Übersicht über die Funktionalität des SMGW mit Zuordnung zu FA-Kategorien, die in ▸Tabelle 3.1 erläutert sind.

Die für die Interoperabilität des SMGW an den Schnittstellen zu verwendenden Kommunikationsprotokolle sind in Kommunikationsszenarien in ▸Abschnitt 4.2, ▸Abschnitt 4.3 und ▸Abschnitt 4.4 beschrieben.

Die Ablehnung syntaktisch nicht korrekter Nachrichten erfolgt durch Anforderungen in den Kommunikationsszenarien, so dass Anforderungen an eine syntaktische Prüfung im FA nicht enthalten sind.

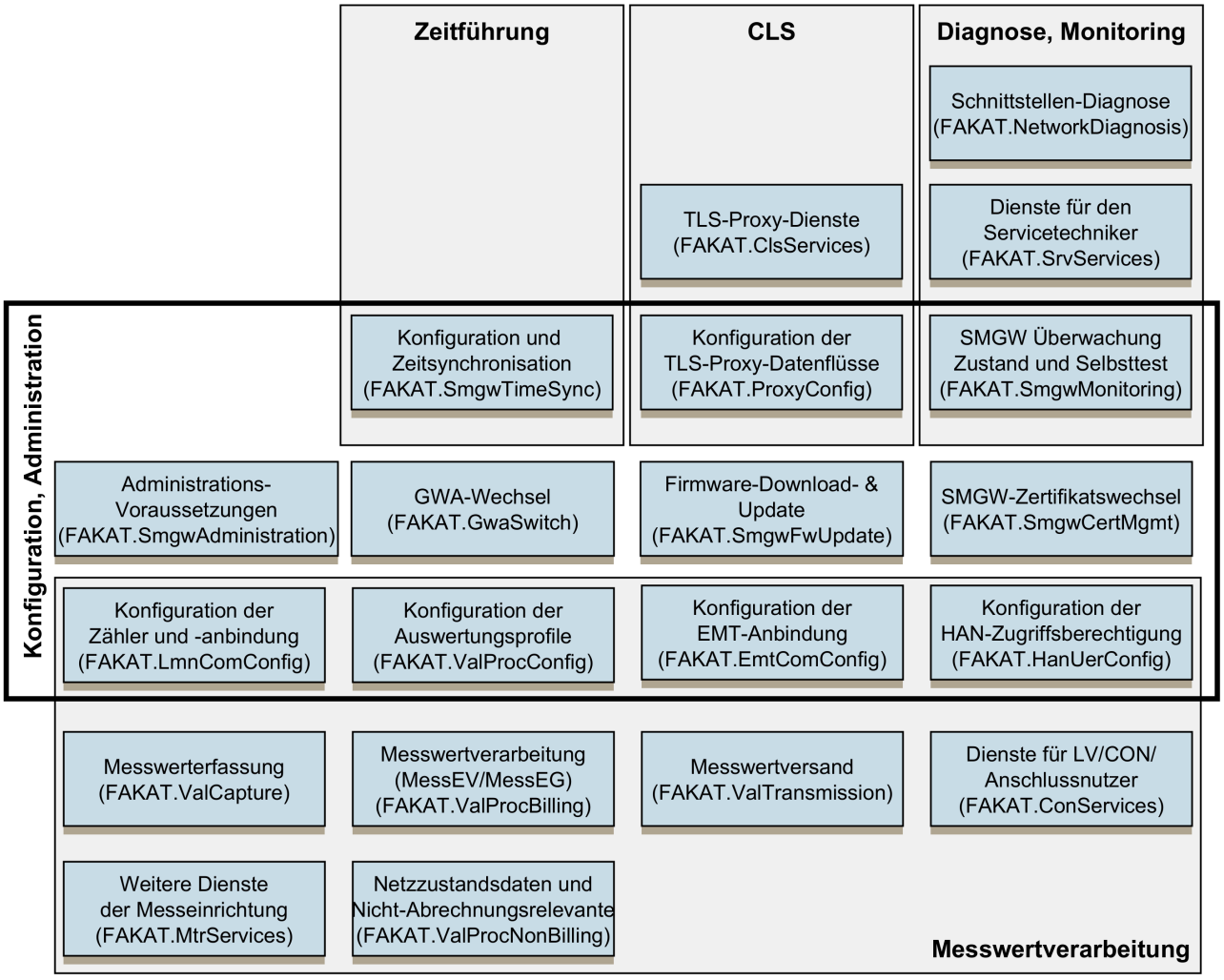


Abbildung 3.1. Funktionsblöcke des SMGW

FA-Kategorien

Beschreibung	Primärer Akteur und Schnittstelle	Abschnitt
Messwertverarbeitung gemäß MessEV/MessEG	SMGW, intern	▸FAKAT.ValProcBilling

Beschreibung	Primärer Akteur und Schnittstelle	Abschnitt
Verarbeitung ohne Messwertbildung gemäß MessEV/MessEG	SMGW, intern	▸FAKAT.ValProcNonBilling
Versand von Messwerten durch das SMGW	EMT, WAN	▸FAKAT.ValTransmission
Erfassung von Messwerten	MTR, LMN	▸FAKAT.ValCapture
Bereitstellung von Diensten für den Anschlussnutzer	CON, HAN	▸FAKAT.ConServices
CLS-Dienste und Proxy-Funktionen des SMGW	CLS, HAN	▸FAKAT.ClsServices
Bereitstellung von Diensten für den Servicetechniker	SRV, HAN	▸FAKAT.SrvServices
Nutzung erweiterter Dienste von Messeinrichtungen	MTR, LMN	▸FAKAT.MtrServices
Zeitführung für das iMSys	SMGW/GWA, WAN	▸FAKAT.SmgwTimeSync
Konfiguration der kommunikativen Anbindung von Messeinrichtungen	GWA, WAN	▸FAKAT.LmnComConfig
Konfiguration der kommunikativen Anbindung von EMT	GWA, WAN	▸FAKAT.EmtComConfig
Konfiguration der kommunikativen Anbindung von HAN-Teilnehmern	GWA, WAN	▸FAKAT.HanUserConfig
Konfiguration der Messwertverarbeitung	GWA, WAN	▸FAKAT.ValProcConfig
Konfiguration der Proxy-Funktion	GWA, WAN	▸FAKAT.ProxyConfig
Diagnose und Monitoring des SMGW	GWA, WAN	▸FAKAT.SmgwMonitoring
Herstellen der Administrationsvoraussetzungen	GWA, WAN	▸FAKAT.SmgwAdministration
GWA-Wechsel	GWA, WAN	▸FAKAT.GwaSwitch
Verwaltung der Zertifikate des SMGW	GWA, WAN	▸FAKAT.SmgwCertMgmt
Firmware-Update des SMGW	GWA, WAN	▸FAKAT.SmgwFwUpdate
Diagnose und Monitoring der Kommunikationsnetzanbindung	GWA, WAN	▸FAKAT.NetworkDiagnosis

Tabelle 3.1 Übersicht über die FA-Kategorien

3.2 Verarbeitung von abrechnungsrelevanten Messwerten (FAKAT.ValProcBilling)

3.2.1 Übersicht

Diese FA-Kategorie enthält die Beschreibung der Tarifanwendungsfälle (TAF) zur Verarbeitung empfangener Messwerte, die zur Abrechnung verwendet werden können.

▸Abbildung 3.2 zeigt den Ablauf der Messwertverarbeitung im SMGW für abrechnungsrelevante Messwerte. Zur Vereinfachung wurden keine Datenflüsse zum Messwertabruf eingezeichnet.

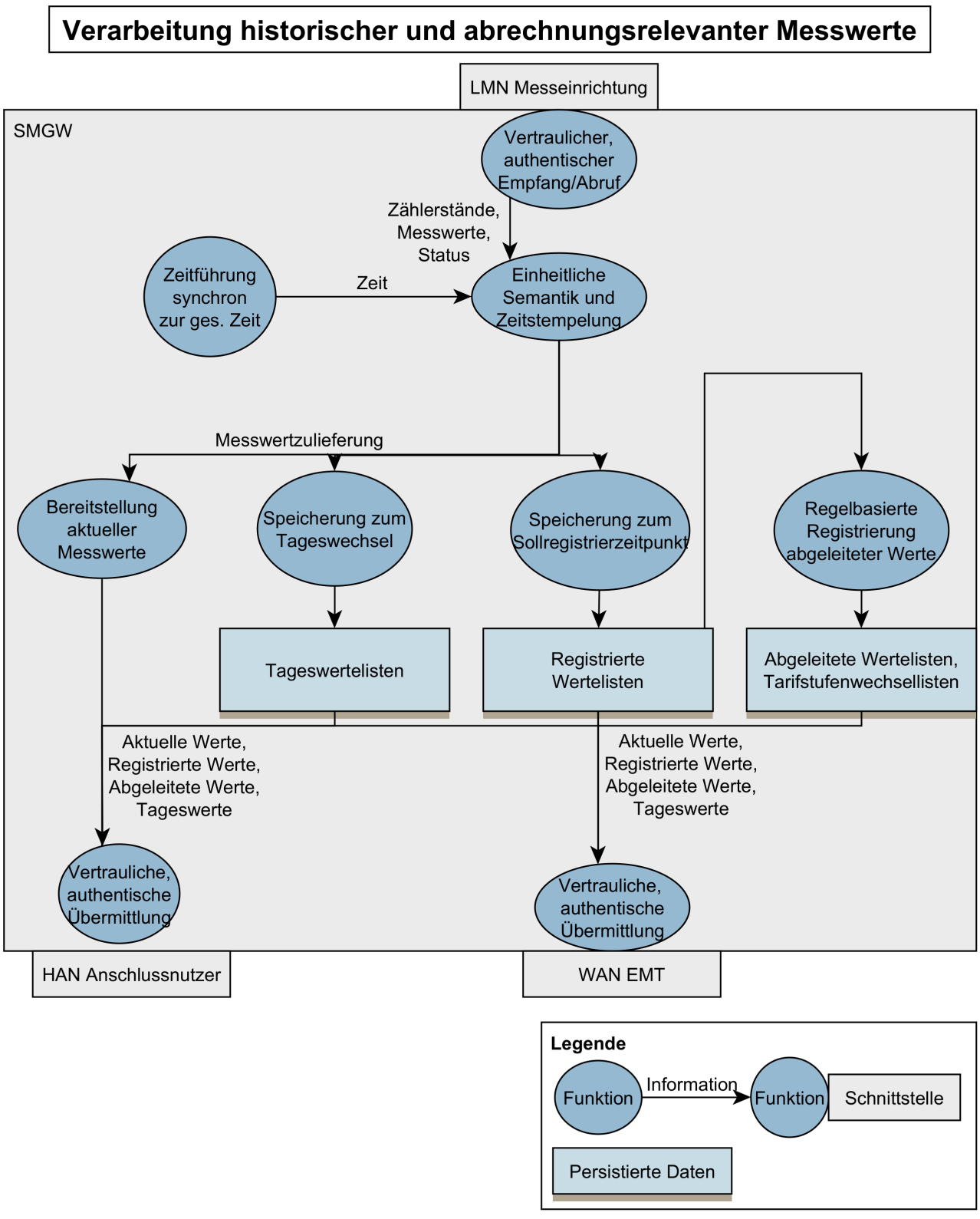


Abbildung 3.2. Ablauf der Messwertverarbeitung für abrechnungsrelevante und historische Messwerte

Von Messeinrichtungen empfangene Nachrichten werden zunächst auf Integrität und Authentizität geprüft und gemäß Anwendungsprotokoll (siehe ▸Abschnitt 4.3) in eine einheitliche Datenstruktur (siehe ▸Eingangsmesswerte) zur Verarbeitung umgesetzt.

Die Verarbeitung abrechnungsrelevanter Messwerte umfasst folgende Schritte:

1. Zeitstempelung der empfangenen Messwerte.

2. Nach der Zeitstempelung erfolgt eine Validierung der Messwerte anhand des Erfassungszeitpunktes und der Statusinformationen der Messeinrichtung und des SMGW.
3. Die validierten Messwerte werden mitsamt der zugehörigen Statusinformationen zum Sollregistrierzeitpunkt in der Liste registrierter Werte (▸RWL) gespeichert.
4. Sofern das SMGW aus den empfangenen Messwerten neue Werte bildet, werden diese Messwerte in einer der Messeinrichtung zugeordneten Liste abgeleiteter Werte (▸AWL) gespeichert und bereitgestellt.

Die Bereitstellung von Daten an der HAN-Schnittstelle für den Anschlussnutzer ist durch ▸FAKAT.ConServices beschrieben. Die Bereitstellung von gespeicherten Werten im Rahmen des Messwertversands an den EMT im WAN ist durch ▸FAKAT.ValTransmission beschrieben.

3.2.2 Übersicht der FA (TAF)

Aufgabe	Umsetzung
TAF1: Datensparsamer Tarif	Das SMGW **MUSS** ▸TAF1 umsetzen. [REQ.FAKAT.ValProcBilling.10]
TAF2: Zeitvariabler Tarif	Das SMGW **MUSS** ▸TAF2 umsetzen. [REQ.FAKAT.ValProcBilling.40]
TAF7: Zählerstandsgangmessung	Das SMGW **MUSS** ▸TAF7 umsetzen. [REQ.FAKAT.ValProcBilling.20]
TAF8: Lastgangbildung mit Maximalwerten	Das SMGW **MUSS+** ▸TAF8 umsetzen. (▸ICS.FAKAT.ValProcBilling.20) [REQ.FAKAT.ValProcBilling.50]
TAF15: Verarbeitung von Messwerten aus registrierenden Messeinrichtungen	Das SMGW **MUSS+** ▸TAF15 umsetzen. (▸ICS.FAKAT.ValProcBilling.20) [REQ.FAKAT.ValProcBilling.30]
Weitere TAF	Das SMGW **KANN** weitere abrechnungsrelevante TAF umsetzen, sofern diese in ergänzenden BSI-Dokumenten zur TR-03109-1 beschrieben sind (▸ICS.FAKAT.ValProcBilling.10). [REQ.FAKAT.ValProcBilling.60]

Tabelle 3.2 Übersicht der FA der Kategorie FAKAT.ValProcBilling

ICS



ICS.FAKAT.ValProcBilling.10

Der GWH **MUSS** im ICS die TAF-Typen auflisten, die über Mindestanforderungen der TR hinaus implementiert sind.



ICS.FAKAT.ValProcBilling.20

Der GWH **MUSS** im ICS erklären, ob die TAF umgesetzt sind.

3.2.3 Datenstrukturen der FA-Kategorie

Die Datenstruktur der RWL und des registrierten Wertes sind in ▸Abschnitt 3.22.35 beschrieben.

Die Datenstruktur der AWL und des abgeleiteten Wertes sind in ▸Abschnitt 3.22.4 beschrieben.

Die Datenstruktur des kombinierten Messwert- und SMGW-Status ist in ▸Abschnitt 3.22.13 beschrieben.

Die Datenstruktur des Messgerätestatus ist in ▸Abschnitt 3.22.28 beschrieben.

Die Datenstruktur des Auswertungsprofils ist in ▸Abschnitt 3.22.6 beschrieben.

Die Datenstruktur des Tarifzustandes ist in ▸Abschnitt 3.22.44 beschrieben.

3.2.4 Registrierung von Messwerten

3.2.4.1 Einleitung

Dieser Abschnitt beschreibt die Anforderungen zur Speicherung von ▸Eingangsmesswerte einer Messeinrichtung in Wertelisten. Die Werteliste enthält in chronologischer Reihenfolge die validierten Zählerstände zum Registrierzeitpunkt, die authentisch und integer von der Messeinrichtung empfangen wurden.

Die registrierte Werteliste (▸RWL) enthält Registrierperioden-synchrone Zeitstempel (▸TAF1, ▸TAF2, ▸TAF7, ▸TAF8). Für ▸TAF15 erfolgt keine Registrierung durch das SMGW, sodass dieser Abschnitt nicht auf ▸TAF15 anzuwenden ist.

Vom GWA konfigurierte Parameter des mit der Messeinrichtung verknüpften Auswertungsprofils bestimmen die Bildung des Registrierzeitstempels:

- Die Registrierperiode (▸TAF1, ▸TAF2, ▸TAF7, ▸TAF8)
- die Berücksichtigung von Aktualitätsinformationen der Messwertnachricht

Formelzeichen	Bedeutung	Bezug
Zeitpunkte		
t_{ref}	Sollregistrierzeitpunkt	t_{SMGW}: ▸refTs in der ▸RWL für ▸TAF1, ▸TAF2, ▸TAF7, ▸TAF8
$t_{measure}$	Messzeitpunkt im Zähler	t_{MTR}: ▸measurementTs in den Eingangsmesswerten
$t_{receive}$	Empfangszeitpunkt im SMGW	t_{SMGW}: ▸receiveTs in den Eingangsmesswerten
Dauern		
T_R	Registrierperiodendauer	"regInterval" der entsprechenden TAF-spezifischen Parameter im Auswertungsprofil ▸TAF1, ▸TAF2, ▸TAF7, ▸TAF8
$T_{L,LKS1}$	Maximale Latenz zwischen Abfrage des SMGW und Empfang im SMGW bei bidirektionaler Kommunikation. Umfasst auch die Integrationszeit zur Bestimmung des Messwertes in der Messeinrichtung.	▸ICS.FA.CaptureRequestedMtrData.10
$T_{L,LKS2}$	Maximale Kommunikationslatenz zwischen Versand aus dem Zähler und Empfang im SMGW bei unidirektionaler Kommunikation	▸ICS.FA.CaptureUnsolicitedRcvdMtrData.10
$T_{Actuality}$	Aktualität: Latenz zwischen Messung und Versand bei unidirektionaler Kommunikation	Aus der empfangenen Messwertnachricht

Tabelle 3.3 Bedeutung der Formelzeichen

Der Sollregistrierzeitpunkt (▸refTs in der ▸RWL) ist der Zeitpunkt (für ▸TAF1, ▸TAF2, ▸TAF7, ▸TAF8), zu dem ein Messwert registriert werden soll. Das SMGW bildet Ist-Registrierzeitstempel (▸ts der ▸RWL) aus dem Empfangszeitstempel des SMGW (▸receiveTs der ▸Eingangsmesswerte) und Aktualitätsinformationen ($T_{Actuality}$) des LMN-Protokolls zur Bestimmung des Messzeitpunktes der Messeinrichtung (▸measurementTs der Eingangsmesswerte). Protokollabhängige Informationen zur Zeitkorrektur Empfangszeitpunkt - Messzeitpunkt sind in [DS] Kapitel "Wireless M-Bus Protokoll" (LKS2 mit "Compact Profile") und [DS] Kapitel "SML" (LKS1) zu finden.

Das SMGW nimmt keine Veränderung der OBIS-Value Group B vor. Es kann daher nicht zwingend anhand der OBIS-Kennzahl erkannt werden, ob die Registrierung des Messwerts in der Messeinrichtung oder im SMGW erfolgt ist. Für den Messwertverwender auf Basis weiterer Informationen in der ▸Exportstruktur erkennbar.

3.2.4.2 Sollregistrierzeitpunkt

Ein Sollregistrierzeitpunkt t_{ref} (in Datenstruktur ▸refTs) ist ein Zeitpunkt mit Datum und sekundengenauer Uhrzeit, dessen Uhrzeit ein Vielfaches auf Basis der Registrierperiode ab der Tageszeit 00:00:00 bildet. Damit hat jeder Sollregistrierzeitpunkt einen konstanten Bezug zu den Referenzzeitpunkten der gesetzlichen Zeit

(HH:00:00 für T_R = 3600s und zusätzlich HH:15:00, HH:30:00, HH:45:00 für T_R = 900s). Die Festlegung sorgt außerdem dafür, dass das Kriterium der maximalen Abweichung zur gesetzlichen Zeit +/-0,03 * T_R implizit eingehalten wird.

Das SMGW bestimmt den Sollregistrierzeitpunkt t_{ref} wie in ▸Tabelle 3.4 dargestellt ausgehen von der aktuellen Systemzeit HH:MM:SS.

Registrierperiode	Aktuelle Systemzeit			Nächster Sollregistrierzeitpunkt
	HH	MM	SS	
15 Minuten	00..23	00..14	00..59	HH:15:00
	00..23	15..29	00..59	HH:30:00
	00..23	30..44	00..59	HH:45:00
	00..22	45..59	00..59	(HH+1):00:00
	23	45..59	00..59	00:00:00 des Folgetages
60 Minuten	00..22	00..59	00..59	(HH+1):00:00
	23	00..59	00..59	00:00:00 des Folgetages
Täglich	▸taf1Pa-rams.endOfDay	00..59	00..59	"endOfDay":00:00 des Folgetages

Tabelle 3.4 Bestimmung des nächsten Sollregistrierzeitpunktes

3.2.4.3 Akzeptanzzeitfenster

Das Akzeptanzzeitfenster beschreibt einen Zeitraum bei der Erfassung von Messwerten im SMGW. Es bestimmt auf Basis der Registrierperiodendauer (▸TAF1, ▸TAF2, ▸TAF7, ▸TAF8) und der Fehlergrenze (1 %) das Zeitfenster um einen Referenzzeitpunkt, in dem eingehende Messwerte rechtzeitig innerhalb der Fehlergrenzen als eingetroffen bewertet werden.

Für Auswertungsprofile, die periodische Sollregistrierzeitpunkte und eine Registrierung im SMGW festlegen (▸TAF1, ▸TAF2, ▸TAF7, ▸TAF8), bestimmt das SMGW das Akzeptanzzeitfenster als [t_{ref} - (0,01*T_R-T_L), t_{ref} + (0,01*T_R)]. Dadurch wird das Akzeptanzfenster auf +/-1 % der Registrierperiodendauer unter Berücksichtigung der Latenz auf dem Übertragungsweg zwischen Messeinrichtung und SMGW eingeschränkt (siehe auch ▸ICS.FA.CaptureRequestedMtrData.10 und ▸ICS.FA.CaptureUnsolicitedRcvdMtrData.10).

Beispiel: Für eine viertelstündliche Registrierperiode (900s) und einer angenommenen Kommunikationslatenz von 2 Sekunden beginnt das Akzeptanzzeitfenster für den Sollregistrierzeitpunkt 0 Uhr um 7 Sekunden vor 0 Uhr und endet um 9 Sekunden nach 0 Uhr.

Das Akzeptanzzeitfenster kann vorzeitig geschlossen werden, sobald Eingangsmesswerte im SMGW erfasst wurden, die näher am Sollregistrierzeitpunkt liegen als alle Messwerte, die möglicherweise noch im verbleibenden Akzeptanzzeitfenster empfangen werden können.

Wird bis zum Zeitpunkt t_{ref} + 0,01*T_R kein Messwert akzeptiert, dann wird der Wert mit ▸smgwStatus.noValue auf "true" in der ▸RWL gespeichert und für den aktuellen Sollregistrierzeitpunkt der letzte registrierte Messwert mit seinem Messzeitpunkt wiederholt. Liegt bisher noch kein Messwert in der ▸RWL vor, wird ein Messwert mit dem Wert "0" und ▸smgwStatus.noValue auf "true" angelegt. Sofern ein LMN-Kommunikationsprofil deaktiviert wurde, werden keine Messwerte akzeptiert.

3.2.4.4 Anforderungen

- (▸tafType="▸TAF1", "▸TAF2", "▸TAF7", "▸TAF8") Das SMGW **MUSS** den (gemäß Systemzeit) am nächsten zum Sollregistrierzeitpunkt (t_{ref}) des "regInterval" (T_R) und im Akzeptanzzeitfenster (Siehe ▸Abschnitt 3.2.4.3) liegenden Messwert für die ▸RWL auswählen. [REQ.FAKAT.ValProcBilling.Registration.10]
- (▸tafType="▸TAF1", "▸TAF2", "▸TAF7", "▸TAF8") Das SMGW **MUSS** den Sollregistrierzeitpunkt gemäß ▸Tabelle 3.4 berechnen. [REQ.FAKAT.ValProcBilling.Registration.80]

- (▸tafType="▸TAF15") Das SMGW **MUSS** den von der Messeinrichtung gebildeten Messzeitpunkt "measurementTs" aus der empfangenen Messwertnachricht als Registrierzeitstempel "ts" in der RWL verwenden. [REQ.FAKAT.ValProcBilling.Registration.30]
- Das SMGW **MUSS** das kombinierte Statuswort (▸Abschnitt 3.22.13) aus SMGW-Status und Status der Messeinrichtung (▸Messgerätestatus) der Eingangsmesswerte (▸Eingangsmesswerte) in die entsprechenden Datenfelder des registrierten Messwerts übernehmen. [REQ.FAKAT.ValProcBilling.Registration.90]
- (▸tafType="▸TAF1", "▸TAF2", "▸TAF7", "▸TAF8") Das SMGW **MUSS** die im Akzeptanzzeitfenster zum Sollregistrierzeitpunkt empfangenen Messwerte in der ▸RWL persistieren, die der Messeinrichtung ▸meterReadingInput.meterId zugeordnet ist. [REQ.FAKAT.ValProcBilling.Registration.40]
- (▸tafType="▸TAF1", "▸TAF2", "▸TAF7", "▸TAF8") Sofern innerhalb des Akzeptanzzeitfensters zum Sollregistrierzeitpunkt kein Messwert empfangen wurde, **MUSS** das SMGW den letzten zu einem Sollregistrierzeitpunkt registrierten Messwert mit seinem Messzeitpunkt für den aktuellen Sollregistrierzeitpunkt wiederholt registrieren und ▸smgwStatus.noValue auf "true" setzen.(▸ICS.FAKAT.ValProcBilling.Registration.10) [REQ.FAKAT.ValProcBilling.Registration.50]
- Wenn innerhalb des Akzeptanzzeitfensters zum Sollregistrierzeitpunkt kein Messwert empfangen wurde und zu den zwei vorherigen Sollregistrierzeitpunkten ebenfalls keine Messwerte vorliegen, dann **MUSS** das SMGW dieses Ereignis protokollieren, sofern am selben Tag nicht bereits eine Protokollierung für die betroffene Messeinrichtung erfolgt ist. ▸ [PTB.1012.1] [REQ.FAKAT.ValProcBilling.Registration.55]
- Sofern im SMGW-Status oder im Messgerätestatus der Eingangsmesswerte (▸Messgerätestatus) das Datenfeld "Status Fataler Fehler" gesetzt ist **MUSS** das SMGW den kombinierten Status zum Sollregistrierzeitpunkt in die Registrierte Werteliste der Messeinrichtung übernehmen und den Fehler für diese "meterId" protokollieren, sofern er für die "meterId" noch nicht protokolliert wurde. ▸ [PTB.1011.2] [REQ.FAKAT.ValProcBilling.Registration.91]
- (▸ICS.MWV.MwStatus.10 gleich "true") Das SMGW **SOLL** die Eingangsmesswerte von Messeinrichtungen nicht in die RWL aufnehmen und nicht verarbeiten, wenn die Messeinrichtung in vorherigen Eingangsmesswerten in "meterStatus" (▸Abschnitt 3.22.28) einen "Status Fataler Fehler" gemeldet hat oder der SMGW-Status "Status Fataler Fehler" anzeigt. [REQ.FA.MeteringValidation.10]
- (▸ICS.MWV.MwStatus.10 gleich "false") Wenn die Messeinrichtung in vorherigen Eingangsmesswerten in "meterStatus" (▸Abschnitt 3.22.28) einen "Status Fataler Fehler" gemeldet hat oder der SMGW-Status "Status Fataler Fehler" anzeigt **MUSS** das SMGW im Kombinierten Statuswort des registrierten Messwerts den Status "Fataler Fehler" setzen. [REQ.FA.MeteringValidation.60]
- Das SMGW **MUSS** die Datenfelder der ▸Eingangsmesswerte gemäß ▸Tabelle 3.5 in die Datenfelder der ▸RWL übernehmen. [REQ.FAKAT.ValProcBilling.Registration.100]
- Das SMGW **MUSS** die Status-Datenfelder der ▸Eingangsmesswerte gemäß ▸Tabelle 3.18 in die Datenfelder der ▸RWL übernehmen. [REQ.FAKAT.ValProcBilling.Registration.120]
- (▸tafType="▸TAF1", "▸TAF2", "▸TAF7", "▸TAF8") Sofern die registrierten Messwerte aufgrund der Parametrierung im ▸Auswertungsprofil nicht für die Abrechnung verwendbar sind ("false" in ▸taf1Params.validatedForBilling, ▸taf2Params.validatedForBilling, ▸taf7Params.validatedForBilling bzw. ▸taf8Params.validatedForBilling), **MUSS** das SMGW ▸smgwStatus.valueNotValidated in der ▸RWL auf "true" setzen. [REQ.FAKAT.ValProcBilling.Registration.130]

Datenfeld der ▸RWL	Ursprung
▸meterId	Entspricht ▸meterId der ▸Eingangsmesswerte.
▸regInterval	Kleinste Registrierperiode aller mit ▸meterReadingInput.meterId verknüpften Auswertungsprofile (Parameter ▸taf1Params.regInterval, ▸taf2Params.regInterval, ▸taf7Params.regInterval bzw. ▸taf8Params.regInterval)
▸columns.obis	▸meterReadingInput.obis aus ▸Auswertungsprofil in Übereinstimmung mit ▸meterReadings.obis der ▸Eingangsmesswerte.
▸columns.unit	▸meterReadings.unit aus den ▸Eingangsmesswerte.
▸refTs	▸TAF1, ▸TAF2, ▸TAF7, ▸TAF8: Sollregistrierzeitpunkt vom SMGW gemäß ▸Abschnitt 3.2.4.2 berechnet.

Datenfeld der ▸RWL	Ursprung
	▸TAF15: die Bestimmung des Sollregistrierzeitpunkts erfolgt durch die Messeinrichtung.
▸ts	▸TAF1, ▸TAF2, ▸TAF7, ▸TAF8: Ist-Registrierzeitpunkt der ▸Eingangsmesswerte bestimmt durch das SMGW.
	▸TAF15: Ist-Registrierzeitpunkt der ▸Eingangsmesswerte bestimmt durch die Messeinrichtung. Üblicherweise identisch mit ▸refTs.
▸values	▸meterReadings.value der ▸Eingangsmesswerte einsortiert in die entsprechend identifizierte Spalte nach ▸columns

Tabelle 3.5 Übernahme von Datenfeldern aus Eingangsmesswerten in RWL

ICS

ICS.MWV.MwStatus.10

Der GWH **MUSS** im ICS angeben, ob das SMGW bei Auftreten eines fatalen Fehlers im Statuswort des Zählers den Messbetrieb für diesen Zähler gemäß ▸REQ.FA.MeteringValidation.10 einstellt ("true") oder Messwerte gemäß ▸REQ.FA.MeteringValidation.60 kennzeichnet ("false").

ICS.FAKAT.ValProcBilling.Registration.10

Der GWH **MUSS** im ICS beschreiben, ob das SMGW außerhalb des Akzeptanzfensters erfasste Messwerte zum Sollregistrierzeitpunkt mit ▸smgwStatus.noValue auf "true" in der ▸RWL speichert.

3.2.4.5 Implementierungshinweise

Wird im Akzeptanzzeitfenster des Sollregistrierzeitpunktes kein Messwert empfangen, werden je nach ▸ICS.FAKAT.ValProcBilling.Registration.10 keine Messwerte an die Messwertverarbeitung zur Registrierung bereitgestellt oder der zuletzt erfasste Messwert wird mit ▸smgwStatus.noValue auf "true" gekennzeichnet und darf nicht zur Abrechnung verwendet werden.

Das SMGW kann Abfragen zu verschiedenen Auslösern zusammenfassen, sofern die Anforderungen verschiedener Auswertungsprofile eingehalten werden.

3.2.5 Erfassung täglicher Verbrauchsinformationswerte

3.2.5.1 Einleitung

Anmerkung

Die täglichen Verbrauchsinformationswerte (Tageswerte der ▸TWL) dienen lediglich der Verbrauchstransparenz des Endkunden und sind nicht für die Abrechnung vorgesehen.

Messwerte auf täglicher Basis zur Abrechnung sind stattdessen immer registrierte Messwerte. Die Registrierperiode entspricht der konfigurierten Registrierperiode (vgl. ▸TAF1). Ein zusätzlicher Messwertabruf des SMGW zum Tageswechsel ist nicht erforderlich, da ein Sollregistrierzeitpunkt immer auf den Tageswechsel fällt.

Die Vorhaltung von Mess- und Registerwerten für den Versand im Bedarfsfall (ehemals ▸TAF6) wird nicht durch eine explizite Liste abgebildet und stellt keinen Verwendungsfall für die ▸TWL dar. Stattdessen werden in ▸FA.DoOnDemandDelivery ausschließlich Anforderungen an deren Bereitstellung gestellt.

Dieser Abschnitt beschreibt die Anforderungen zur Übernahme von ▸Eingangsmesswerte einer Messeinrichtung in die Tageswerteliste (▸TWL). Die Erfassung von Tageswerten erfolgt für Messeinrichtungen, die durch ▸TAF1, ▸TAF2, ▸TAF7, ▸TAF8 oder ▸TAF15 verwendet werden.

Die ▸TWL enthält in chronologischer Reihenfolge die historischen Zählerstände der mit der ▸TWL über den Parameter ▸meterReadingInput.meterId verknüpften Messeinrichtung zum Tageswechsel (im ▸Auswertungsprofil durch den GWA konfiguriert). Die Differenz der Zählerstände zwischen zwei Zeitpunkten der

▸TWL erlaubt dem Endkunden die Bestimmung der Energie- oder Wasserverbrauchsinformation eines Zeitraumes (z.B. Jahr, Monat, Woche).

Parameter des mit der Messeinrichtung über ▸meterReadingInput.meterId verknüpften Auswertungsprofils bestimmen die zu erfassenden Messgrößen (Parameter ▸meterReadingInput.obis).

Die in der ▸TWL erfassten Messwerte stellen eine tägliche Messwertwiederholung der Anzeige der Messeinrichtung dar. Die Erfassungszeitpunkte der ▸TWL sind nicht notwendigerweise synchron zu Registrierzeitpunkten des SMGW. Die Einhaltung von zeitlichen Fehlergrenzen gemäß [MessEV]/[MessEG] wird nicht geprüft.

3.2.5.2 Anforderungen

Das SMGW **MUSS** die über ▸meterReadingInput.obis im ▸Auswertungsprofil referenzierten Messwerte zum Tageswechselzeitpunkt (Parameter ▸taf1Params.endOfDay, ▸taf2Params.endOfDay, ▸taf7Params.endOfDay, ▸taf8Params.endOfDay bzw. ▸taf15Params.endOfDay) in der ▸TWL der Messeinrichtung gemäß ▸meterReadingInput.meterId persistieren. [REQ.FAKAT.ValProcDaily.Capturing.10]

Das SMGW **MUSS** die Datenfelder der ▸Eingangsmesswerte gemäß ▸Tabelle 3.6 in die Datenfelder der ▸TWL übernehmen. Dabei ist die Zuordnung der OBIS-IDs der ▸Eingangsmesswerte zu den Spalten der ▸TWL zu beachten. [REQ.FAKAT.ValProcDaily.Capturing.30]

Das SMGW **MUSS** die Status-Datenfelder der ▸Eingangsmesswerte gemäß ▸Tabelle 3.18 in die Datenfelder der ▸TWL übernehmen. [REQ.FAKAT.ValProcDaily.Capturing.50]

Liegt zum Sollregistrierzeitpunkt des Tageswechsels kein Zählerstand vor, **SOLL** das SMGW den am nächsten zum Tageswechselzeitpunkt in der Messeinrichtung gebildeten Zählerstand in die TWL übernehmen. (▸ICS.FAKAT.ValProcDaily.10, ▸ICS.FAKAT.ValProcDaily.20) [REQ.FAKAT.ValProcDaily.Capturing.60]

Datenfeld der ▸TWL	Ursprung
▸meterId	Entspricht ▸meterId der ▸Eingangsmesswerte
▸columns.obis	▸meterReadings.obis der ▸Eingangsmesswerte in Übereinstimmung mit dem ▸Auswertungsprofil.
▸columns.unit	▸meterReadings.unit der ▸Eingangsmesswerte in Übereinstimmung mit dem ▸Auswertungsprofil.
▸refTs	▸TAF1: Tagesende ("HH":00:00) mit "HH"= ▸taf1Params.endOfDay
	▸TAF2: Tagesende ("HH":00:00) mit "HH"= ▸taf2Params.endOfDay
	▸TAF7: Tagesende ("HH":00:00) mit "HH"= ▸taf7Params.endOfDay
	▸TAF8: Tagesende ("HH":00:00) mit "HH"= ▸taf8Params.endOfDay
	▸TAF15: Tagesende ("HH":00:00) mit "HH"= ▸taf15Params.endOfDay
	Für alle TAF gilt, dass die Zeitinformation in UTC mit Information zum Bezug zur lokalen Zeit kodiert wird.
▸ts	▸ts der ▸Eingangsmesswerte als Mess- bzw. Empfangszeitpunkt durch das SMGW bestimmt (Zeitinformation in UTC mit Information zum Bezug zur lokalen Zeit)
▸measurementTs	▸measurementTs der ▸Eingangsmesswerte, sofern vorhanden
▸values	▸meterReadings.value der ▸Eingangsmesswerte einsortiert in die entsprechend identifizierte Spalte nach ▸columns

Tabelle 3.6 Übernahme von Datenfeldern aus Eingangsmesswerten in TWL

ICS



ICS.FAKAT.ValProcDaily.10

Der GWH **MUSS** im ICS angeben, ob das SMGW die Tageswerte aus der RWL entnimmt. Liegt zum Sollregistrierzeitpunkt zum Tageswechsel kein Zählerstand vor, fehlt der Tageswert.

ICS.FAKAT.ValProcDaily.20

(▸ICS.FAKAT.ValProcDaily.10 gleich "false") Der GWH **MUSS** im ICS angeben (in Sekunden), in welchem Akzeptanzfenster um den Tageswechselzeitpunkt die Zeitstempel der Tageswerte erfasst werden. Ein Wert 1800 bedeutet, dass ein Zählerstand mit Zeitstempel frühestens eine halbe Stunde vor bis spätestens eine halbe Stunde nach Tageswechsel in der TWL gespeichert wird.

3.2.5.3 Implementierungshinweise

Sofern die Registrierperiode der entsprechenden ▸RWL es zulässt, können innerhalb der Implementierung die registrierten Werte auch als Tageswerte verwendet und ausgegeben werden. Hierbei ist zu bedenken, dass die Vorhaltefristen bei ▸RWL und ▸TWL unterschiedlich sind (siehe ▸Abschnitt 5.5). Dies sollte bei der internen Speicherung und Verwaltung der Werte bedacht werden.

3.2.6 Gestufte Kumulation von Energiemengen

3.2.6.1 Einleitung

Dieser Abschnitt beschreibt die Anforderungen zur Bildung abgeleiteter Werte durch Kumulation von Energiemengen, die aus der Differenz von zwei Zählerständen zwischen zwei Zeitpunkten gebildet werden. Zum Zeitpunkt der Berechnung gilt eine Tarifstufe, die das aktive Register bestimmt. Der Zeitpunkt eines Wechsels der Tarifstufe wird als Tarifumschaltzeitpunkt bezeichnet.

Für die Anforderungen in diesem Abschnitt gelten folgende Festlegungen:

- Sei Z_n ein Messwert zum Zeitpunkt t_n gemäß der Berechnungsgrundlage in ▸Tabelle 3.7.
- Sei t_m ein Zeitpunkt vor dem Zeitpunkt t_n.
- Sei t_{latest} immer der jüngste Zeitpunkt in der Vergangenheit ausgehend von der Systemzeit, der der Definition gemäß t_n entspricht. Dadurch wird immer der Zeitpunkt des neusten Messwerts markiert (gilt auch bei Messwerten mit ▸combinedStatus ="MISSING_VALUE").
- Sei Z_{n-1} ein Messwert zum Zeitpunkt t_{n-1}, wobei t_{n-1} der direkte Vorgänger von t_n gemäß der Berechnungsgrundlage in ▸Tabelle 3.7 ist.
- Sei *Register X* das für den Zeitraum $[t_m, t_n]$ bestimmte, aktive Register auf Basis der Festlegung in ▸Tabelle 3.7 mit $X \in [1, 62]$.
- Sei *Register 63* das Fehlerregister, das alle Energiemengen vorhält, die nicht eindeutig einem *Register X* zugeordnet werden können. Die Fehlerbehandlung basiert auf dem kombinierten Messgeräte- und SMGW-Statuswort (Siehe ▸Abschnitt 3.5.4.3).
- Sei *Register 0* das Gesamtregister, das die gesamten kumulierten Energiemengen aller *Register X* und von *Register 63* vorhält.

▸Tabelle 3.7 stellt für alle kumulierenden TAF dar, welche Messwerte als Grundlage für die Berechnung von Energiemengen verwendet werden und wie die aktive Tarifstufe und damit das aktive Register festgelegt wird.

TAF	Berechnungsgrundlage	Festlegung aktives Register
▸TAF2	• Bestimmung von Energiemengen als Differenz zweier Zählerstände aus der ▸RWL gemäß ▸meterReadingInput.meterId im ▸Auswertungsprofil. • Berechnung der Energiemengen und Zuordnung zum aktiven Register erfolgt zum Vorliegen eines Wertes zu jedem Sollregistrierzeitpunkt t_n der ▸RWL. • Messwerte Z_n für die Berechnung werden von Sollregistrierzeitpunkten t_n aus der ▸RWL genommen.	• Statische Konfiguration im ▸Auswertungsprofil für Tarifumschaltzeitpunkte auf Basis von Zeitbedingungen legen das aktive Register fest. • Tarifumschaltzeitpunkte entweder auf Basis einer Zählzeitdefinition (▸taf2Params.timeOfUseDefinition) oder auf Basis von Zeitplänen (▸taf2Params.switchTimetable) definieren jederzeit genau ein aktives Register. • Jeder Tarifumschaltzeitpunkt fällt immer auf einen Sollregistrierzeitpunkt gemäß der als Berechnungsgrundlage verwendeten ▸RWL.

Tabelle 3.7 Berechnungsbasis und Registerfestlegung nach TAF

Zum Gültigkeitsbeginn des Auswertungsprofils (▸validityPeriod.from) werden die Register für Energiemengen auf "0" gesetzt. Während der Gültigkeit des Auswertungsprofils werden die Energiemengen im jeweils aktiven Register kumuliert. Energiemengen, die nicht eindeutig zugeordnet werden können, werden in ein Fehlerregister kumuliert. Darüber hinaus werden alle Energiemengen zusätzlich in ein Gesamtregister kumuliert.

Bei Erreichen des Abrechnungsturnus (▸taf2Params.billingInterval) wird der Stand der Register für Energiemengen in der ▸AWL fixiert und exportiert.

Die ▸AWL enthält die chronologisch sortierten, fixierten Registerstände zum Ende des vergangenen Abrechnungsturnus. Der letzte Eintrag der ▸AWL wird mit jedem empfangenen Messwert zum Sollregistrierzeitpunkt aktualisiert. Zum nächsten Ende des Abrechnungsturnus werden diese aktuellen Registerstände in der ▸AWL fixiert.

Für die lokale Bereitstellung der Energiemengenregister (siehe ▸FA.ExportDerivedMtrReading) wird die Aktualisierung der Energiemengenregister bei Empfang von Zählerständen auch zwischen zwei Sollregistrierzeitpunkten durchgeführt.

3.2.6.2 Anforderungen

- Das SMGW **MUSS** zum Beginn des Gültigkeitszeitraums (▸validityPeriod.from) für alle abgeleiteten Register der zugehörigen ▸AWL den Wert "0" in ▸values.value eintragen [REQ.FAKAT.ValProcBilling.Accumulation.10]
- Das SMGW **MUSS** das *Register X* für den jeweiligen Zeitraum $[t_m, t_n]$ auf Basis der Parametrierung im ▸Auswertungsprofil und der Beschreibung in ▸Tabelle 3.7 bestimmen. [REQ.FAKAT.ValProcBilling.Accumulation.20]
- Das SMGW **MUSS** die Berechnung der Energiemengen gemäß ▸Tabelle 3.8 bei jeder Änderung von t_{latest} durchführen. [REQ.FAKAT.ValProcBilling.Accumulation.30]
- Sofern die zur Berechnung der Energiemengen verwendeten Messwerte nicht für die Abrechnung verwendbar sind (▸smgwStatus.valueNotValidated), **MUSS** das SMGW den entsprechenden Status im ▸smgwStatus.valueNotValidated in der zugehörigen ▸AWL auf "1" setzen. [REQ.FAKAT.ValProcBilling.Accumulation.40]

#	Zu erfüllende Bedingungen (Und-verknüpft)	Berechnung Energiemenge	Zielregister
1	• Z_{latest} hat ▸combinedStatus = "NO_ERROR" oder "WARNING" • $Z_{latest-1}$ hat ▸combinedStatus = "NO_ERROR" oder "WARNING"	$Z_{latest} - Z_{latest-1}$	• *Register X* • *Register 0*
2	• Z_{latest} hat ▸combinedStatus = "MISSING_VALUE"	0	• keins, da "0"
	Informative Erläuterung: fehlt der neuste Messwert findet keine Veränderung der Register statt.		
3	• Z_{latest} hat ▸combinedStatus = "NO_ERROR" oder "WARNING" • Z_m hat ▸combinedStatus = "NO_ERROR" oder "WARNING" • Alle Werte im Intervall $[t_{m+1}, t_{latest-1}]$ haben ▸combinedStatus = "MISSING_VALUE" • Es gibt mindestens einen Messwert im Intervall $[t_{m+1}, t_{latest-1}]$ • Im Intervall $[t_{m+1}, t_{latest-1}]$ liegt kein Tarifumschaltzeitpunkt	$Z_{latest} - Z_m$	• *Register X* • *Register 0*
	Informative Erläuterung: bei fehlenden vergangenen Messwerten innerhalb derselben Tarifstufe ist die eindeutige Zuordnung zu einem *Register X* und damit die Kumulierung bei Eintreffen eines Messwerts dennoch möglich.		
4	• Z_{latest} hat ▸combinedStatus = "NO_ERROR" oder "WARNING" • Z_m hat ▸combinedStatus = "NO_ERROR" oder "WARNING" • Alle Messwerte im Intervall $[t_{m+1}, t_{latest-1}]$ haben ▸combinedStatus = "MISSING_VALUE" • Es gibt mindestens einen Messwert im Intervall $[t_{m+1}, t_{latest-1}]$ • Im Intervall $[t_{m+1}, t_{latest-1}]$ liegt mindestens ein Tarifumschaltzeitpunkt	$Z_{latest} - Z_m$	• *Register 63* • *Register 0*

#	Zu erfüllende Bedingungen (Und-verknüpft)	Berechnung Energiemenge	Zielregister
	Informative Erläuterung: bei fehlenden vergangenen Messwerten und stattfindendem Tarifstufenwechsel ist keine eindeutige Zuordnung zu einem *Register X* bei Eintreffen eines Messwerts möglich, weshalb ins Fehlerregister kumuliert wird.		
5	• Z_{latest} hat ▸combinedStatus = "TEMPORARY_ERROR" oder "PERMANENT_ERROR" • Z_m hat ▸combinedStatus = "NO_ERROR", "WARNING" oder "TEMPORARY_ERROR" • Alle Messwerte im Intervall $[t_{m+1}, t_{latest-1}]$ haben ▸combinedStatus = "MISSING_VALUE"	$Z_{latest} - Z_m$	• *Register 63* • *Register 0*
	Informative Erläuterung: bei einem gestörten Messwert oder dem ersten Auftreten eines permanenten Fehlers wird die Differenz zum letzten nicht fehlenden Messwert unabhängig seines Status ins Fehlerregister kumuliert. Dazwischen liegende Tarifumschaltzeitpunkte spielen dabei keine Rolle.		
6	• Z_{latest} hat ▸combinedStatus = "PERMANENT_ERROR" • Z_m hat ▸combinedStatus = "PERMANENT_ERROR" • Alle Messwerte im Intervall $[t_{m+1}, t_{latest-1}]$ haben ▸combinedStatus = "MISSING_VALUE"	$Z_{latest} - Z_m$	• *Register 63* • *Register 0*
	Informative Erläuterung: nachdem zuvor ein permanenter Fehler aufgetreten ist, werden keine Messwerte registriert oder sind danach ebenfalls mit permanentem Fehler markiert. Differenzen werden dann nur noch ins Gesamt- und ins Fehlerregister kumuliert.		

Tabelle 3.8 Kumulation in verschiedenen Fällen

3.2.7 Ableitung von Leistungsmittel- und -maximalwerten

3.2.7.1 Einleitung

Dieser Abschnitt beschreibt die Anforderungen zur Bildung abgeleiteter Werte für einen Lastgang. Ein Lastgang ist eine Zeitreihe aus mittleren Leistungen einer Lastgangperiode. Die mittlere Leistung bestimmt sich aus der Energiemenge, die innerhalb einer Lastgangperiode angefallen ist, multipliziert mit einem Faktor abhängig von der Lastgangperiodendauer. Die für die Lastgangberechnung zugrundeliegenden Messwerte sind in der dem Zähler zugeordneten RWL gespeichert. Der berechnete Lastgang und der Maximumwert wird in der AWL gespeichert.

Sollen mehrere Lastgänge für einen Zähler mit unterschiedlichen Messgrößen berechnet werden (z.B. Zweirichtungs- oder Vierquadrantenzähler), so sind mehrere TAF8-Auswertungsprofile zu konfigurieren.

Registrier- und Lastgangperiode

Die Lastgangperiodendauer entspricht immer der Registrierperiodendauer.

Die Registrierperiode wird für die Bestimmung der Leistungsmaximalwerte im Abrechnungsturnus benötigt. Die Lastgangperiode bestimmt den zeitlichen Abstand der in der AWL gebildeten Leistungsmittelwerte.



Abbildung 3.3. Beispiel für Ableitung des Lastgangs und Bestimmung des Leistungsmaximalwerts

Lastgangberechnung

Es gelten folgende Festlegungen:

- t_{n-1} und t_n Zeitpunkt zum Beginn und Ende einer Lastgangperiode. Beide fallen auf einen Sollregistrierzeitpunkt (siehe ▸Abschnitt 3.2.4.2).
- Z_n, Z_{n-1} Register: Der in der RWL registrierte Zählerstand zum Beginn und Ende der Lastgangperiode (einschließlich Messgerätestatuswort).
- $c_{E,P}$() Umrechnungsfaktor Energiemenge in mittlere Leistung.
  - Für Energiemenge kWh, s in Sekunden, P in kW ist $c_{E,P}$(kWh,kW,s) = 3600.
  - Für Energiemenge in Wh, s in Sekunden, P in W ist $c_{E,P}$(Wh,W,s) = 3600.
- $P_{avg,l}(t_n)$ Register: Die mittlere Leistung der Lastgangperiode zum Zeitpunkt t_n berechnet sich zu

  $$P_{t_n} = \frac{(Z_n - Z_{n-1}) * c_{E,P}}{t_n - t_{n-1}}$$

  Dieser Wert wird zum Ende der Lastgangperiode in der AWL aktualisiert.

Maximumbildung

Für den Abrechnungsturnus (siehe ▸taf8Params.reportingPeriod) wird zusätzlich der Maximalwert der mittleren Leistung über alle Registrierperioden bestimmt.

Der Maximalwert wird in jeder Registrierperiode bestimmt.

Es gelten folgende Festlegungen:

- $P_{avg,r}$ ist die mittlere Leistung der letzten Registrierperiode.
- $P_{max}(t_n)$ Register: Zum Ende der Registrierperiode (t_n) aktualisierte Maximalleistung in der laufenden Abrechnungsperiode mit dem Zeitpunkt t_{max} des Leistungsmaximums. P_{max} wird aktualisiert, wenn $P_{avg,r} > P_{max}$ ist.

Dieser Wert wird zum Ende der Lastgangperiode in der AWL fixiert.

Fehlerbehandlung

Die Fehlerbehandlung basiert auf dem kombinierten Messgeräte- und SMGW-Statuswort (Siehe ▸Abschnitt 3.5.4.3).

Liegt für den Zeitpunkt t_n (Ende der Lastgangperiode) oder t_{n-1} (Beginn der Lastgangperiode) kein Zählerstand Z vor ("MISSING_VALUE") oder ist der Messgerätestatus gleich "TEMPORARY_ERROR" oder "PERMANENT_ERROR", so wird als abgeleiteter Wert $P_{avg,l}(t_n)$ zum Ende der Lastgangperiode die mittlere Leistung "0" für die Lastgangperiode gespeichert und im Kombinierten Statuswort das zum letzten Registrierzeitpunkt empfangene Messgerätestatuswort zum ▸smgwStatus.noValue bzw. "MISSING_VALUE" in die ▸AWL übernommen.

Der Wert kann nicht zur Abrechnung verwendet werden. Die Information aus dem Kombinierten Statuswort kann beim Messwertempfänger als Hinweis für eine Ersatzwertbildung des oder der fehlenden Lastgangwerte verwendet werden.

Momentanwertberechnung

Ergänzend wird für den lokalen Nutzer bei jedem Empfang eines Zählerstandes die mittlere Leistung der aktuellen Lastgangperiode berechnet.

Es gelten folgende Festlegungen:

- $P_{avg,latest}$ Register: Mittlere Leistung der laufenden Registrierperiode beim letzten empfangenen Zählerstand

$$P_{avg,latest} = \frac{(Z_{latest} - Z_{n-1}) * c_{E,P}}{t_{latest} - t_{n-1}}$$

Dieser Wert wird nur lokal bereitgestellt und nicht in der AWL persistiert.

3.2.7.2 Anforderungen

- Das SMGW **MUSS** zum Beginn des Abrechnungsturnus das Leistungsmaximalwertregister "P_{max}" in ▸AWL auf den Wert "0" setzen. [REQ.FAKAT.ValProcBilling.DerivePower.10]
- Das SMGW **MUSS** die Berechnung von $P_{avg,l}$(t_n) gemäß ▸Tabelle 3.9 jeweils zu den auf einen Sollregistrierzeitpunkt fallenden Zeitpunkten der Lastgangperiode gemäß ▸taf8Params.regInterval durchführen und in der AWL persistieren. [REQ.FAKAT.ValProcBilling.DerivePower.20]
- Das SMGW **MUSS** die Berechnung von P_{max}/t_{max} gemäß ▸Tabelle 3.9 jeweils zu den Registrierzeitpunkten gemäß ▸Abschnitt 3.2.4 durchführen und am Ende der Abrechnungsperiode gemäß ▸taf8Params.reportingPeriod in der AWL persistieren. [REQ.FAKAT.ValProcBilling.DerivePower.25]
- Das SMGW **MUSS** die Berechnung von $P_{avg,latest}$ jeweils beim Empfang eines Zählerstandes durchführen. [REQ.FAKAT.ValProcBilling.DerivePower.30]
- Sofern die zur Berechnung der Energiemengen verwendeten Messwerte nicht für die Abrechnung verwendbar sind (▸smgwStatus.valueNotValidated), **MUSS** das SMGW den entsprechenden Status im ▸smgwStatus.valueNotValidated in der zugehörigen ▸AWL auf "1" setzen. [REQ.FAKAT.ValProcBilling.DerivePower.40]
- Das SMGW **MUSS** gewährleisten, dass die Auflösung der berechneten Leistung P_{avg} gegenüber der Zahl der signifikanten Stellen der Eingangsmesswerte (Z) nicht verschlechtert wird. Dabei ist die niederwertigste signifikante Stelle nach der Division kaufmännisch zu runden. [REQ.FAKAT.ValProcBilling.DerivePower.50]

#	Zu erfüllende Bedingungen (Und-verknüpft)	Zielregister
1	• Z_n hat ▸combinedStatus = "NO_ERROR" oder "WARNING" • Z_{n-1} hat ▸combinedStatus = "NO_ERROR" oder "WARNING" • $P_{avg,r} > P_{max}$	Setze P_{max} gleich P_{avg} und t_{max} gleich t_n
2	• Z_n hat ▸combinedStatus = "NO_ERROR" oder "WARNING" • Z_{n-1} hat ▸combinedStatus = "NO_ERROR" oder "WARNING"	$SetzeP_{t_n}gleich\frac{(Z_n - Z_{n-1}) * c_{E,P}}{t_n - t_{n-1}}$
3	Z_n oder Z_{n-1} hat ▸combinedStatus = "MISSING_VALUE" oder "TEMPORARY_ERROR" oder "PERMANENT_ERROR"	Setze $P_{avg,l}(t_n)$ gleich "0". P_{max} und t_{max} wird nicht verändert.

#	Zu erfüllende Bedingungen (Und-verknüpft)	Zielregister
	Informative Erläuterung: Nur wenn zu Beginn und Ende der Lastgangperiode ein gültiger Zählerstand registriert wurde, kann Pavg,l berechnet werden. Anderenfalls wird zum Ende der Lastgangperiode wird $P_{avg,l}$ "MISSING_VALUE" registriert und der Maximalwert nicht verändert..	
4	Z_n hat ▸combinedStatus = "PERMANENT_ERROR"	Setze $P_{avg,l}(t_n)$ gleich "0". P_{max} und t_{max} wird nicht verändert.
	Informative Erläuterung: Nachdem zuvor ein permanenter Fehler aufgetreten ist, sind alle nicht fehlenden Messwerte danach ebenfalls mit permanentem Fehler markiert. Das Register $P_{avg,l}(t)$ wird bis zum Ende der Abrechnungsperiode "0" und $P_{max}(t)$ wird bis zum Ende der Abrechnungsperiode nicht mehr verändert.	

Tabelle 3.9 Aktualisierung der abgeleiteten Werteregister

3.2.8 TAF1: Datensparsamer Tarif

3.2.8.1 Beschreibung

Dieser Anwendungsfall erlaubt die Erfassung und Versendung von Zählerständen elektrischer Energie, thermischer Energie, sowie von Zählerständen von Gas- und Wasservolumen, 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 Werte, Auswertungen über das Verbrauchsverhalten des Anschlussnutzers getätigt werden können. Es wird dabei nur eine Tarifstufe betrachtet. ▸Tabelle 3.10 zeigt einen beispielhaften Ausschnitt eine Liste von Messwerten, die im Rahmen dieses TAF versandt werden könnte.

Der TAF kann für die Verarbeitung von Zählerständen für elektrische Energie, Gas, Wasser und Wärmeenergie konfiguriert werden. Der TAF verarbeitet die registrierten Werte aus der RWL. Es werden keine abgeleiteten Werte berechnet. Der TAF versendet dazu aus den registrierten Messwerten jeweils einen Wert zu jeder parametrierten Messgröße zu Beginn der Gültigkeitsdauer (Erstauslesung), periodisch monatlich und zum Ende der Gültigkeitsdauer (Endablesung). Die konfigurierbaren Messgrößen sind die Zeitintegrale (Zählerstände) für elektrische Energie, thermische Energie, sowie Gas- und Wasservolumen.

Aktuelle Zählerstände, die registrierten Messwerte aus der RWL und die Zählerstände zum Tageswechsel werden dem über das Auswertungsprofil zugeordneten Anschlussnutzer bzw. Anlagenbetreiber lokal bereitgestellt.

Zeitstempel	Zählerstand in kWh
01.02.2022 0:00:00h	512
01.03.2022 0:00:00h	545
01.04.2022 0:00:00h	567
01.05.2022 0:00:00h	577
...	...

Tabelle 3.10 Beispiel für einen einfachen Tarif mit minimalem Datenversand bei monatlicher Abrechnung

3.2.8.2 Anforderungen

Dieser TAF unterscheidet sich lediglich in Details von den anderen TAF aus ▸FAKAT.ValProcBilling. Da der technische Ablauf sonst identisch ist, wird an dieser Stelle stattdessen auf die relevanten Abschnitte verwiesen:

- Die Prüfung der Parametrierung des SMGW erfolgt im Rahmen von Anforderungen in ▸FAKAT.ValProcConfig.
- Der Empfang beziehungsweise Abruf von Messwerten der Messeinrichtung auf Basis der im Auswertungsprofil angegebenen Registrierperiode ("regInterval") wird in ▸FAKAT.ValCapture beschrieben.
- Die Bildung von registrierten Werten (siehe ▸RWL) einschließlich der notwendigen Prüfungen vom Status des SMGW und der Messeinrichtung wird in ▸Abschnitt 3.2.4 beschrieben.
- Die Auslösung des Nicht-Turnus-Versands zum Stichtag oder nach Kommunikationsstörung ist in ▸FAKAT.ValProcConfig beschrieben.

- Die Bildung von informativen Tageswerten (siehe ▸TWL) wird in ▸Abschnitt 3.2.5 beschrieben.
- Die Auswahl von registrierten Werten, die zum Versand herangezogen werden sollen, und die Durchführung des Versands wird in ▸FAKAT.ValTransmission beschrieben.
- Die Erst- und Endablesung wird in ▸FAKAT.ValTransmission beschrieben.
- Die Bereitstellung von Messwerten und Informationen zu diesem TAF für den Anschlussnutzer wird in ▸FAKAT.ConServices beschrieben.
- Die Benachrichtigung des Anschlussnutzers über Parametrierung und Änderungen dieses TAF wird durch zu protokollierende Ereignisse in ▸FAKAT.ValProcConfig beschrieben.

3.2.9 TAF2: Zeitvariabler Tarif



Anmerkung

Die in diesem Anwendungsfall zu parametrierenden Tarifumschaltzeitpunkte können auf zwei verschiedene Arten festgelegt werden:

- Verwendung von Zählzeitdefinitionen (▸taf2Params.timeOfUseDefinition): Paare aus Zeitpunkten und Tarifstufen definieren lückenlos das aktive Register.
- Verwendung von Zeitplänen (▸taf2Params.switchTimetable): Listen von Zeitplänen für Saison, Woche, Tag und Uhrzeit definieren lückenlos das aktive Register.

Die Verwendung der Zählzeitdefinition wird empfohlen. Zeitpläne werden als mögliche Parametrierung in einer zukünftigen Version entfallen und werden nicht im Rahmen der Konformitätsprüfung bewertet.

3.2.9.1 Beschreibung

Dieser Anwendungsfall ermöglicht es, elektrische Energiemengen in Abhängigkeit der Zeit in unterschiedlichen Registern zu erfassen. Hiermit können zeitvariable Tarife realisiert werden, bei denen bezogene oder gelieferte Energie nach Tageszeit oder Tag in Tarifstufen differenziert wird. Je Tarifstufe kann ein unterschiedlicher Preis in Rechnung gestellt werden.

Das SMGW kumuliert die anfallenden Energiemengen[1] seit Beginn des Abrechnungszeitraumes in dem jeweils aktiven Zählregister. Auf diese Weise wird die gesamte, innerhalb des Abrechnungszeitraumes angefallene Energiemenge auf die Register verteilt. Die Energiemenge wird aus der Differenz zwischen zwei Zählerständen in das aktive Zählregister kumuliert (siehe ▸Abschnitt 3.2.6) und als abgeleiteter Wert persistiert.

Das SMGW stellt dem Anschlussnutzer zu diesem Anwendungsfall an der HAN-Schnittstelle den aktuellen Zählerstand, die registrierten und abgeleiteten Wertelisten (▸RWL, ▸AWL), die aktuelle Tarifstufe und über das UserLog die historischen Tarifumschaltzeitpunkte bereit.

Sofern die den Tarifstufen zugeordneten Preisbestandteile konfiguriert wurden (Parameter ▸taf2Params.cost), stellt das SMGW diese dem Anschlussnutzer bereit. Das SMGW wertet die Preisbestandteile nicht aus.

▸Abbildung 3.4 stellt die Energiemengenzuordnung für einen zeitvariablen Tarif mit zwei Tarifstufen dar.

[1] Die Energiemenge entspricht der über die Zeit integrierten Leistung.

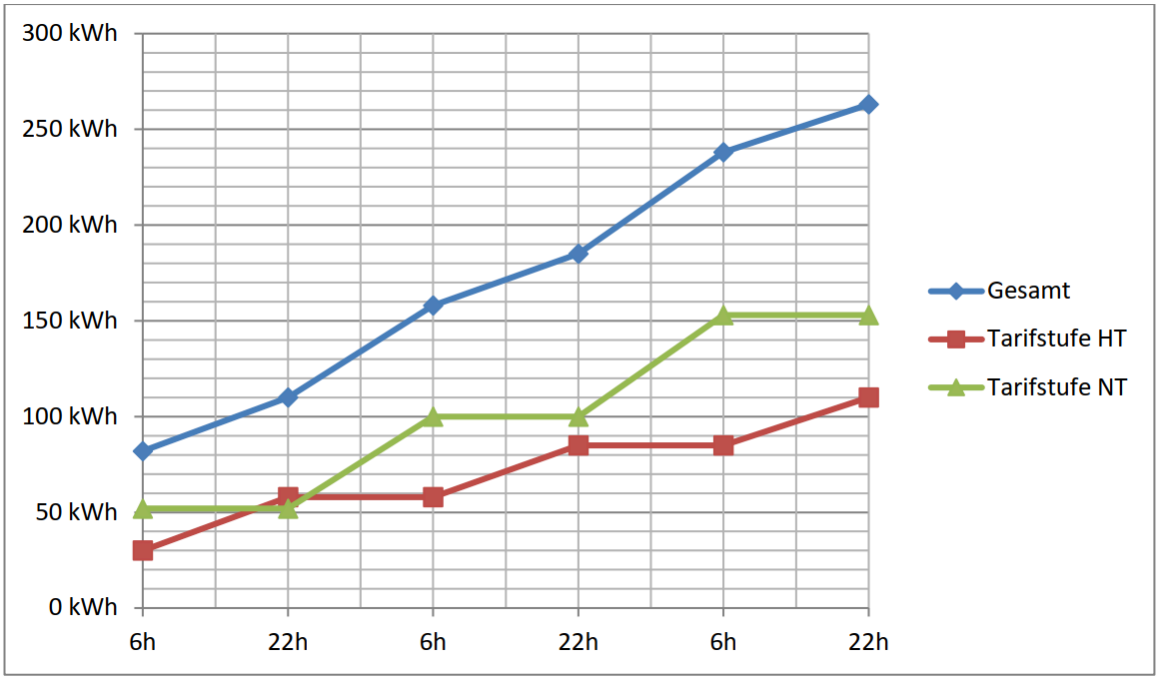


Abbildung 3.4. Beispiel für einen zeitvariablen Tarif mit zwei Tarifstufen (HT/NT)

▸Abbildung 3.5 stellt Ablauf der Messwertverarbeitung für den zeitvariablen Tarif dar. Dies stellt eine graphische Darstellung der Anforderungen aus ▸Abschnitt 3.2.6 dar.

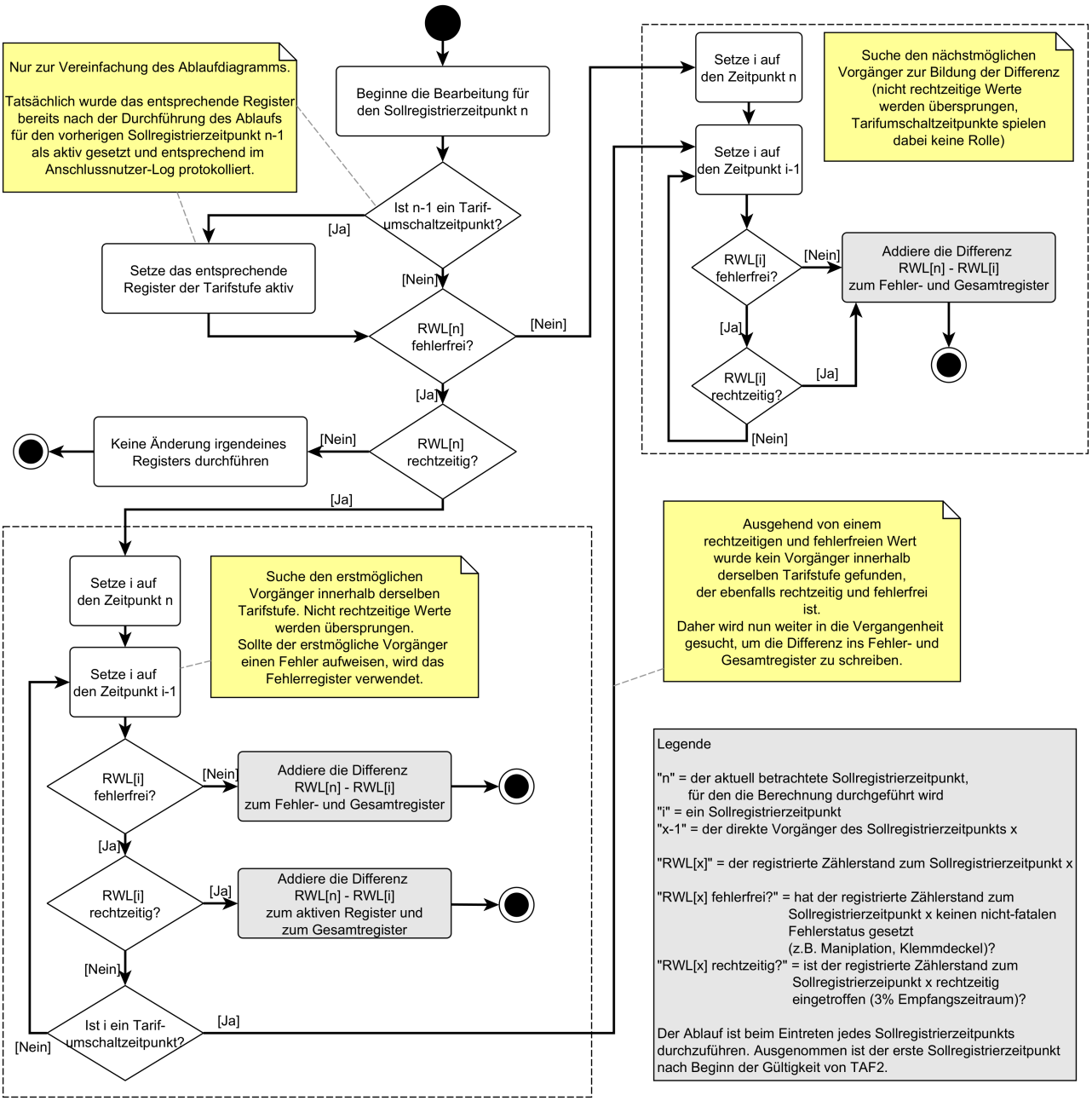


Abbildung 3.5. Ablaufdiagramm für TAF2

3.2.9.2 Anforderungen

Dieser TAF basiert auf einer registrierperiodenbasierten Erfassung von Zählerständen und unterscheidet sich durch die zeitliche Zuordnung und Berechnung von Energiemengen von den anderen TAF aus ▸FAKAT.ValProcBilling. An dieser Stelle wird auf die für diesen TAF relevanten Abschnitte der Technischen Richtlinie verwiesen:

- Die Prüfung der Parametrierung des SMGW erfolgt im Rahmen von Anforderungen in ▸FAKAT.ValProcConfig.
- Der Empfang beziehungsweise Abruf von Messwerten der Messeinrichtung auf Basis der im Auswertungsprofil angegebenen Registrierperiode (▸taf2Params.regInterval) wird in ▸FAKAT.ValCapture beschrieben.
- Die Bildung von registrierten Werten der ▸RWL einschließlich der notwendigen Prüfungen vom Status des SMGW und der Messeinrichtung wird in ▸Abschnitt 3.2.4 beschrieben.
- Die Bildung von abgeleiteten, kumulierten Energiemengen der ▸AWL einschließlich der notwendigen Fehlerbehandlungen durch das SMGW wird in ▸Abschnitt 3.2.6 beschrieben.

- Die Auslösung des Nicht-Turnus-Versands zum Stichtag oder nach Kommunikationsstörung ist in ▸FAKAT.ValProcConfig beschrieben.
- Die Bildung von informativen Tageswerten (siehe ▸TWL) wird in ▸Abschnitt 3.2.5 beschrieben.
- Die Durchführung des Versands abgeleiteter Werte wird in ▸FAKAT.ValTransmission beschrieben.
- Die Erst- und Endablesung wird in ▸FAKAT.ValTransmission beschrieben.
- Die Bereitstellung von Messwerten und Informationen zu diesem TAF für den Anschlussnutzer wird in ▸FAKAT.ConServices beschrieben.
- Die Benachrichtigung des Anschlussnutzers über Parametrierung und Änderungen dieses TAF wird durch zu protokollierende Ereignisse in ▸FAKAT.ValProcConfig beschrieben.

3.2.10 TAF6: Abruf von Messwerten im Bedarfsfall

Dieser Anwendungsfall wird nun über ▸FA.DoOnDemandDelivery in ▸Abschnitt 3.4.6 abgedeckt und ist daher an dieser Stelle nicht weiter beschrieben.

3.2.11 TAF7: Zählerstandsgangmessung

3.2.11.1 Beschreibung

Dieser Anwendungsfall erlaubt die Erfassung und Versendung von Zählerstandsgängen elektrischer Energie, thermischer Energie, sowie von Zählerstandsgängen von Gas- und Wasservolumen. Über diesen Anwendungsfall ist zudem eine zentrale Tarifierung durch den EMT möglich.

Im Zusammenhang mit durch den EMT tarifierten Energiemengen sind die eichrechtlichen Anforderungen nach MessEG und MessEV zu beachten.

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.

Die Zählerstandsgänge haben eine konstante, konfigurierte Registrierperiodenlänge von 15 oder 60 Minuten.

Aktuelle Zählerstände, die Registrierten Messwerte und die Zählerstände zum Tageswechsel werden dem über das Auswertungsprofil zugeordneten Anschlussnutzer bzw. Anlagenbetreiber lokal bereitgestellt.

3.2.11.2 Anforderungen

Dieser TAF unterscheidet sich lediglich in Details von den anderen TAF aus ▸FAKAT.ValProcBilling. Da der technische Ablauf sonst identisch ist, wird an dieser Stelle stattdessen auf die relevanten Abschnitte verwiesen:

- Die Prüfung der Parametrierung des SMGW erfolgt im Rahmen von Anforderungen in ▸FAKAT.ValProcConfig.
- Der Empfang beziehungsweise Abruf von Messwerten der Messeinrichtung auf Basis der im Auswertungsprofil angegebenen Registrierperiode ("regInterval") wird in ▸FAKAT.ValCapture beschrieben.
- Die Bildung von registrierten Werten (siehe ▸RWL) einschließlich der notwendigen Prüfungen vom Status des SMGW und der Messeinrichtung wird in ▸Abschnitt 3.2.4 beschrieben.
- Die Auslösung des Nicht-Turnus-Versands zum Stichtag oder nach Kommunikationsstörung ist in ▸FAKAT.ValProcConfig beschrieben.
- Die Bildung von informativen Tageswerten (siehe ▸TWL) wird in ▸Abschnitt 3.2.5 beschrieben.
- Die Auswahl von registrierten Werten, die zum Versand herangezogen werden sollen, und die Durchführung des Versands wird in ▸FAKAT.ValTransmission beschrieben.
- Die Erst- und Endablesung wird in ▸FAKAT.ValTransmission beschrieben.
- Die Bereitstellung von Messwerten und Informationen zu diesem TAF für den Anschlussnutzer wird in ▸FAKAT.ConServices beschrieben.

- Die Benachrichtigung des Anschlussnutzers über Parametrierung und Änderungen dieses TAF wird durch zu protokollierende Ereignisse in ▸FAKAT.ValProcConfig beschrieben.

3.2.12 TAF8: Lastgangmessung mit Maximumbestimmung

3.2.12.1 Beschreibung

Dieser Anwendungsfall erlaubt die Berechnung von Lastgängen aus registrierten Zählerständen elektrischer Energie und bestimmt pro Abrechnungsperiode zusätzlich die Maximalleistung.

Der Anwendungsfall ermöglicht neben der Erfassung von Verbrauchsleistungen analog auch die Erfassung von Einspeiseleistungen. In diesem Fall liefert der Zähler Messwerte für eingespeiste Energie anstatt für verbrauchte Energie.

Die Lastgänge haben eine konstante, konfigurierte Periodenlänge von 5, 15 oder 60 Minuten.

Der Anwendungsfall verarbeitet die im SMGW registrierten Zählerstände. Wird der Lastgang oder Maximalwert in einer registrierenden Messeinrichtung gebildet, muss ▸TAF15 zur Erfassung der in der Messeinrichtung registrierten Messwerte konfiguriert werden.

3.2.12.2 Anforderungen

Dieser TAF unterscheidet sich in der Bestimmung der abgeleiteten Werte von den anderen TAF aus ▸FAKAT.ValProcBilling. Da der technische Ablauf sonst identisch ist, wird an dieser Stelle stattdessen auf die relevanten Abschnitte verwiesen:

- Die Prüfung der Parametrierung des SMGW erfolgt im Rahmen von Anforderungen in ▸FAKAT.ValProcConfig.
- Der Empfang beziehungsweise Abruf von Messwerten der Messeinrichtung auf Basis der im Auswertungsprofil angegebenen Registrierperiode ("regInterval") wird in ▸FAKAT.ValCapture beschrieben.
- Die Bildung von registrierten Werten (siehe ▸Registrierter Wert und registrierte Wertliste (RWL)) einschließlich der notwendigen Prüfungen vom Status des SMGW und der Messeinrichtung wird in ▸Abschnitt 3.2.4 beschrieben.
- Die Berechnung von abgeleiteten Werten (mittlere Leistung und Leistungsmaximalwert) auf der Basis der registrierten Werten wird in ▸Abschnitt 3.2.7 beschrieben.
- Die Auslösung des Nicht-Turnus Versands zum Stichtag oder nach Kommunikationsstörung ist in ▸FAKAT.ValProcConfig beschrieben.
- Die Bildung von Tageswerten (siehe ▸TWL) wird in ▸Abschnitt 3.2.5 beschrieben.
- Die Auswahl von abgeleiteten Werten, die zum Versand herangezogen werden sollen, und die Durchführung des Versands wird in ▸FAKAT.ValTransmission beschrieben.
- Die Erst- und Endablesung wird in ▸FAKAT.ValTransmission beschrieben.
- Die Bereitstellung von Messwerten und Informationen zu diesem TAF für den Anschlussnutzer wird in ▸FAKAT.ConServices beschrieben.
- Die Benachrichtigung des Anschlussnutzers über Parametrierung und Änderungen dieses TAF wird durch zu protokollierende Ereignisse in ▸FAKAT.ValProcConfig beschrieben.

3.2.13 TAF15: Verarbeitung von in Messeinrichtungen registrierten Messwerten

3.2.13.1 Beschreibung

Dieser Anwendungsfall erlaubt die Erfassung, lokale Bereitstellung und Versendung von Zählerständen die in einer registrierenden Messeinrichtung gebildet wurden. Die Registrierende Messeinrichtung registriert die integrierten elektrischen Energiemengen, thermischen Energiemengen, sowie Gas- und Wasservolumenmengen in äquidistanten Zeitintervallen (Registrierperioden). Die zeitliche Einhaltung der Registrierperiodendauer und des Registrierzeitpunktes obliegt der Messeinrichtung. Das SMGW stellt der Messeinrichtung periodisch die mit der gesetzlichen Zeit synchronisierte Systemzeit des SMGW authentisch bereit (siehe ▸FA.ExportTimeToMtr).

Ein Zählerstands- oder Lastgang enthält eine Reihe von chronologisch geordneten Registerwerten zu Registrierzeitpunkten in einem einheitlichen zeitlichen Abstand.

Bei einem **Zählerstandsgang** wird dabei im Register das Zeitintegral seit Herstellung des Zählers abgebildet, bei einem Lastgang wird das Zeitintegral seit Beginn des letzten Registrierzeitpunktes abgebildet. Für Energie stellt ein Zählerstandsgang somit für jeden Registrierzeitpunkt die gemessene Energiemenge seit Herstellung des Zählers dar. Die Differenz von zwei Zählerständen ergibt die gemessene Energiemenge zwischen den Zeitpunkten.

Bei einem **Lastgang** beginnt das Zeitintegral bei jedem Registrierzeitpunkt erneut. Der Registrierte Messwert enthält somit die gemessene Energiemenge seit letztem Registrierzeitpunkt. Durch Division der Energiemenge der jeweiligen Registrierperiode durch die Registrierperiodendauer wird die mittlere Leistung der Registrierperiode berechnet.

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.

Durch Konfiguration der für die Messwertverarbeitung zu verwendenden OBIS-IDs im Auswertungsprofil legt der GWA fest, ob vom Zähler übermittelte Zählerstände oder Lastgänge/Zählerstandsdifferenzen erfasst werden. GWA, MSB und EMT (Marktteilnehmer) vereinbaren die zu konfigurierenden OBIS-IDs. So sind gemäß ▸Abschnitt 2.5.2 beispielsweise für elektrische Energie OBIS-IDs 1-0:C.8.0 (für Zählerstandsgänge) oder 1-0:C.29.0 (für Lastgänge) zu konfigurieren und für Gas OBIS-IDs 7-0:3.[0,1].0 (für Zählerstandsgänge) oder 7-0:99.21.[15,16,17] (für Lastgänge) zu konfigurieren.

Messwerte werden im SMGW erfasst und gespeichert, jedoch nicht erneut registriert. Zur Gewährleistung der Interoperabilität zur Verwendung der Messwerte an der HAN- und WAN-Schnittstelle werden die von der Messeinrichtung registrierten Werte in einer Registrierten Werteliste durch das SMGW bereitgestellt.

Die periodisch von der Messeinrichtung abgerufenen Momentanwerte werden dem Anlagenbetreiber oder Anschlussnutzer an der HAN-Schnittstelle unverzüglich nach Erfassung durch das SMGW bereitgestellt (Siehe ▸FA.ReadInstantMtrReading).

Das SMGW versendet die im Abrechnungsturnus (siehe ▸taf15Params.billingInterval) erfassten Zählerstandsgänge oder Lastgänge gemäß Versandzeitpunkt ▸meterDataOutput.trigger.deliveryTime an den im Auswertungsprofil benannten EMT.

3.2.13.2 Anforderungen

Im Unterschied zu anderen TAFs in ▸FAKAT.ValProcBilling ist die Einhaltung von Registrierzeitpunkten und zeitlichen Fehlergrenzen durch die Messeinrichtung zu gewährleisten. Da der technische Ablauf sonst identisch ist, wird an dieser Stelle stattdessen auf die relevanten Abschnitte verwiesen:

- Die Prüfung der Parametrierung des SMGW erfolgt im Rahmen von Anforderungen in ▸FAKAT.ValProcConfig.
- Der Empfang beziehungsweise Abruf von Messwerten der Messeinrichtung wird in ▸FA.CaptureRegisteredValues beschrieben.
- Die Auslösung des Nicht-Turnus Versands oder nach Kommunikationsstörung ist in ▸FAKAT.ValProcConfig beschrieben.
- Die Bildung von Tageswerten (siehe ▸TWL) wird in ▸Abschnitt 3.2.5 beschrieben.
- Die Auswahl von registrierten Werten, die zum Versand herangezogen werden sollen, und die Durchführung des Versands wird in ▸FAKAT.ValTransmission beschrieben.
- Die Erst- und Endablesung wird in ▸FAKAT.ValTransmission beschrieben.
- Die Bereitstellung von Messwerten und Informationen zu diesem TAF für den Anschlussnutzer wird in ▸FAKAT.ConServices beschrieben.
- Die Benachrichtigung des Anschlussnutzers über Parametrierung und Änderungen dieses TAF wird durch zu protokollierende Ereignisse in ▸FAKAT.ValProcConfig beschrieben.

3.3 Verarbeitung von nicht-abrechnungsrelevanten Messwerten (FAKAT.ValProcNonBilling)

3.3.1 Übersicht

Diese FA-Kategorie enthält Tarifanwendungsfälle für die Verarbeitung von Messwerten, die nicht zur Verwendung gemäß MessEV/MessEG vorgesehen sind.

Abbildung 3.6 zeigt den Ablauf der Messwertverarbeitung im SMGW für nicht MessEV/MessEG-relevante Netzzustandsdaten und Momentanwerte. Zur Vereinfachung wurden keine Datenflüsse zum Messwertabruf eingezeichnet.

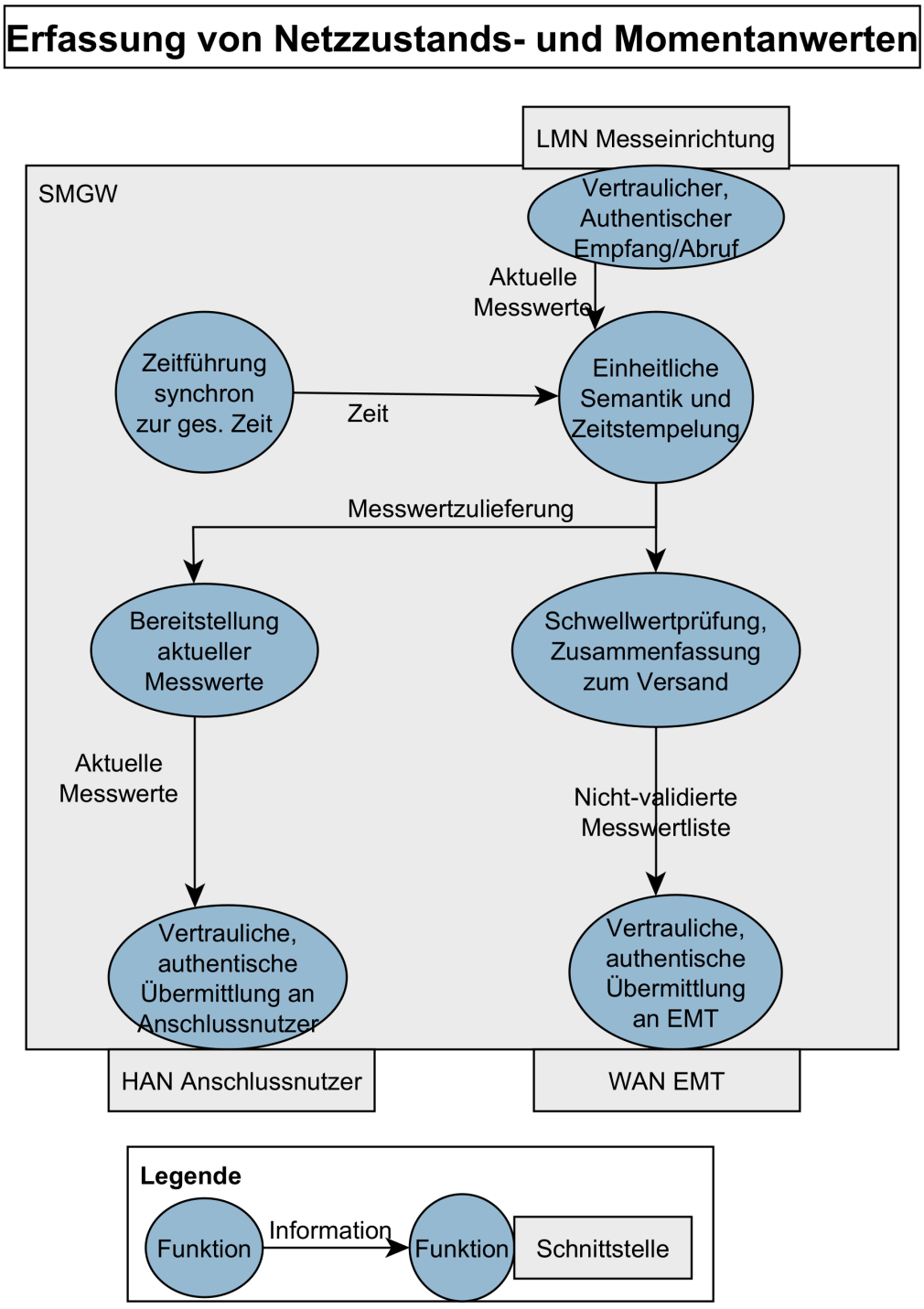


Abbildung 3.6. Ablauf der Messwertverarbeitung für Netzzustandsdaten und Momentanwerte

3.3.2 Übersicht der FA (TAF)

Aufgabe	Umsetzung
TAF9: Abruf der Ist-Einspeisung	Das SMGW **MUSS** ▸TAF9 umsetzen. [REQ.FAKAT.ValProcNonBilling.10]
TAF10: Abruf von Netzzustandsdaten	Das SMGW **MUSS** ▸TAF10 umsetzen [REQ.FAKAT.ValProcNonBilling.20]
TAF14: Hochfrequente Messwertbereitstellung für Mehrwertdienste	Das SMGW **MUSS** ▸TAF14 umsetzen. [REQ.FAKAT.ValProcNonBilling.30]
Weitere TAF	Das SMGW **KANN** weitere nicht-abrechnungsrelevante TAF umsetzen, sofern diese in ergänzenden BSI-Dokumenten zur TR-03109-1 beschrieben sind (▸ICS.FAKAT.ValProcNonBilling.10). [REQ.FAKAT.ValProcNonBilling.40]

Tabelle 3.11 Übersicht der FA der Kategorie FAKAT.ValProcNonBilling

ICS



ICS.FAKAT.ValProcNonBilling.10

Der GWH **MUSS** im ICS die nicht-abrechnungsrelevanten TAF-Typen auflisten, die über Mindestanforderungen der TR hinaus implementiert sind.

3.3.3 Datenstrukturen der FA-Kategorie

Die Datenstrukturen der nichtvalidierten Messwertliste und des nichtvalidierten Messwertes sind in ▸Abschnitt 3.22.33 beschrieben.

Die Datenstruktur der Eingangsmesswerte ist in ▸Abschnitt 3.22.5 beschrieben.

3.3.4 Erfassung von nicht qualitativ validierten Messwerten

3.3.4.1 Einleitung

Dieser Abschnitt beschreibt die Anforderungen zur Übernahme der ▸Eingangsmesswerte einer Messeinrichtung in die Werteliste für nicht qualitativ validierten Messwerten (▸NWL). Die ▸NWL enthält in chronologischer Reihenfolge aktuelle Messwerte, für die folgende Eigenschaften gelten:

- Der Zeitstempel besitzt keinen Bezug zu Registrierzeitpunkten.
- Die Messwerte sind nicht monoton steigend.
- Die Messwerte werden nicht auf Einhaltung von Zeit- oder Werte-Fehlergrenzen geprüft.

Damit kann die Erfassung der Messwerte auch bei Statuswechseln oder Grenzwertverletzungen erfolgen. Die untere Grenze der Erfassungsfrequenz der Messgrößen wird durch die Abtastrate der Messeinrichtung, die Kommunikationslatenz und die Erfassungsperiode im ▸Auswertungsprofil bestimmt.

Der Parameter ▸meterReadingInput.obis im ▸Auswertungsprofil bestimmt die zu erfassenden Messgrößen der verknüpften Messeinrichtung.

Die in der ▸NWL erfassten Messwerte sind nicht für die Abrechnung gemäß [MessEV]/[MessEG] zu verwenden.

3.3.4.2 Anforderungen

- Sofern die ▸meterId der ▸Eingangsmesswerte über mindestens ein ▸Auswertungsprofil mit Erfassungsperiode (▸taf9Params.capPeriod, ▸taf10Params.capPeriod oder ▸taf14Params.capPeriod) ungleich "0" referenziert ist, **MUSS** das SMGW die über ▸meterReadingInput.obis referenzierten Messwerte in der ▸NWL der Messeinrichtung speichern. [REQ.FAKAT.ValProcNonBilling.Capturing.10]
- Das SMGW **MUSS** die Datenfelder der ▸Eingangsmesswerte gemäß ▸Tabelle 3.12 in die Datenfelder der ▸NWL übernehmen. Dabei ist die Zuordnung der ▸meterReadings.obis der ▸Eingangsmesswerte zu den Spalten der ▸NWL zu beachten. [REQ.FAKAT.ValProcNonBilling.Capturing.30]

- (Parameter ▸taf9Params.preprocessing) gleich "SIGN_INVERT") Das SMGW **SOLL** das Vorzeichen der Momentanleistungswerte aus ▸Eingangsmesswerte bei der Übernahme in die ▸NWL invertieren. (▸ICS.FAKAT.ValProcNonBilling.Capturing.20) [REQ.FAKAT.ValProcNonBilling.Capturing.40] [2]
- (Parameter ▸taf9Params.preprocessing) gleich "CONSUMPTION_CAP") Das SMGW **SOLL** das die positiven Momentanleistungswerte ▸Eingangsmesswerte vor der Übernahme in die ▸NWL auf den Wert "0" setzen. (▸ICS.FAKAT.ValProcNonBilling.Capturing.20) [REQ.FAKAT.ValProcNonBilling.Capturing.50] [3]
- Das SMGW **MUSS** die Status-Datenfelder der ▸Eingangsmesswerte aus ▸meterStatus gemäß ▸Tabelle 3.18 in die Datenfelder der ▸NWL (▸combinedStatus) übernehmen. [REQ.FAKAT.ValProcNonBilling.Capturing.60]
- Das SMGW **SOLL** je Messeinrichtung 1440 Messwertsätze für bis zu 16 Messgrößen vorhalten können (▸ICS.FAKAT.ValProcNonBilling.Capturing.10). [REQ.FAKAT.ValProcNonBilling.Capturing.70]

Datenfeld der ▸NWL	Ursprung
▸meterId	Entspricht ▸meterId der ▸Eingangsmesswerte
▸columns.obis	▸meterReadingInput.obis aus ▸Auswertungsprofil in Übereinstimmung mit ▸meterReadings.obis der ▸Eingangsmesswerte.
▸columns.unit	Einheitenzeichen und Einheitenvorsatzzeichen gemäß ▸Abschnitt 2.5.2 für die jeweilige Messgröße in Übereinstimmung des Einheitenzeichens mit ▸meterReadings.unit der ▸Eingangsmesswerte. Sofern sich durch Skalierung auf das Einheitenvorsatzzeichen eine Anpassung des Dezimalexponent des Wertes ergibt, ist eine entsprechende Dezimalpunktverschiebung durchzuführen.
▸ts	▸ts Mess- bzw. Empfangszeitpunkt der ▸Eingangsmesswerte
▸values.value	▸meterReadings.value der ▸Eingangsmesswerte einsortiert in die entsprechend identifizierte Spalte nach ▸columns

Tabelle 3.12 Übernahme von Datenfeldern aus Eingangsmesswerten in NWL

ICS



ICS.FAKAT.ValProcNonBilling.Capturing.10

Der GWH **MUSS** im ICS deklarieren welche Mindestzahl von Messwertsätzen je Messeinrichtung das SMGW in der NWL (Ringspeicher) vorgehalten kann, bevor Messwertsätze verdrängt werden.



ICS.FAKAT.ValProcNonBilling.Capturing.20

Der GWH **MUSS** im ICS deklarieren welche der Funktionen CONSUMPTION_CAP, SIGN_INVERT implementiert sind.

3.3.4.3 Implementierungshinweise

Die ▸NWL ist als Ringspeicher implementierbar, der nur der Zwischenspeicherung zwischen Erfassung und Versand der Messwerte dient.

Sofern der Hersteller geplante Neustarts für das SMGW vorsieht, sollten noch nicht versandte Messwerte der NWL aufbewahrt werden.

3.3.5 TAF9: Bereitstellung der Ist-Einspeisung einer Erzeugungsanlage

3.3.5.1 Beschreibung

Dieser Anwendungsfall erlaubt die Erfassung und Bereitstellung der momentanen Ist-Einspeiseleistung nach dem Erneuerbare-Energien-Gesetz und dem Kraft-Wärme-Kopplungsgesetz. Das SMGW versendet dazu periodisch, bei Bedarf auf Verlangen des berechtigten Empfängers (ausgelöst durch den GWA) oder bei Verlet-

[2] Bei Zweirichtungszählern ist die Einspeiseleistung ein negativer Wert. Durch die Vorzeichenumkehr wird ein positiver Wert an den EMT übermittelt.

[3] Damit werden bei Zweirichtungszählern im Falle einer Ist-Einspeisemessung die Verbrauchsinformationen aus den Momentanwerten (Leistung, Strom) entfernt.

zung festgelegter Schwellwerte ausgewählte Werte an die berechtigten Empfänger. Aktuelle Messwerte der Ist-Einspeiseleistung werden dem über das Auswertungsprofil zugeordneten Anschlussnutzer bzw. Anlagenbetreiber lokal bereitgestellt.

3.3.5.2 Anforderungen

Dieser TAF unterscheidet sich lediglich im Verwendungszweck und den zulässigen Messgrößen von anderen TAF aus ▸FAKAT.ValProcNonBilling. Da der technische Ablauf sonst identisch ist, wird an dieser Stelle stattdessen auf die relevanten Abschnitte verwiesen:

- Die Einschränkung der zulässigen Messgrößen für diesen TAF wird im Rahmen von Anforderungen an die Parametrierung in ▸FAKAT.ValProcConfig beschrieben.
- Der Empfang beziehungsweise Abruf von Messwerten der Messeinrichtung auf Basis der im Auswertungsprofil angegebenen Erfassungsperiode wird in ▸FAKAT.ValCapture beschrieben.
- Die Bildung und Zusammenfassung zu nicht-validierten Messwerten (siehe ▸NWL) für den Messwertversand wird in den generellen Anforderungen von ▸FAKAT.ValProcNonBilling beschrieben.
- Der Versand der nicht-validierten Messwerte wird in ▸FAKAT.ValTransmission beschrieben.
- Der lokale Abruf von Informationen zu diesem TAF für den Anschlussnutzer bzw. Anlagenbetreiber wird in ▸FAKAT.ConServices beschrieben.
- Die Benachrichtigung des Anschlussnutzers über die Parametrierung dieses TAF wird durch zu protokollierende Ereignisse in ▸FAKAT.ValProcConfig beschrieben.

3.3.6 TAF10: Abruf von Netzzustandsdaten

3.3.6.1 Beschreibung

Dieser Anwendungsfall ermöglicht die Erfassung und Bereitstellung von Netzzustandsdaten aus dem SMGW an den Netzbetreiber. Aktuelle Messwerte der Netzzustandsdaten werden dem über das Auswertungsprofil zugeordneten Anschlussnutzer bzw. Anlagenbetreiber lokal bereitgestellt.

Sofern es aufgrund gesetzlicher Regelungen erforderlich ist, können Netzzustandsdaten im Rahmen des Versands pseudonymisiert werden (s. ▸FA.ExportNonAccntMtrReading), wenn im Auswertungsprofil ein Pseudonym parametriert ist.

3.3.6.2 Anforderungen

Dieser TAF unterscheidet sich lediglich im Verwendungszweck und den zulässigen Messgrößen von anderen TAF aus ▸FAKAT.ValProcNonBilling. Da der technische Ablauf sonst identisch ist, wird an dieser Stelle stattdessen auf die relevanten Abschnitte verwiesen:

- Die Einschränkung der zulässigen Messgrößen für diesen TAF wird im Rahmen von Anforderungen an die Parametrierung in ▸FAKAT.ValProcConfig beschrieben.
- Der Empfang beziehungsweise Abruf von Messwerten der Messeinrichtung auf Basis der im Auswertungsprofil angegebenen Erfassungsperiode wird in ▸FAKAT.ValCapture beschrieben.
- Die Bildung und Zusammenfassung zu nicht-validierten Messwerten (siehe ▸NWL) für den Messwertversand wird in den generellen Anforderungen von ▸FAKAT.ValProcNonBilling beschrieben.
- Der Versand der nicht-validierten Messwerte wird in ▸FAKAT.ValTransmission beschrieben.
- Der lokale Abruf von Informationen zu diesem TAF für den Anschlussnutzer bzw. Anlagenbetreiber wird in ▸FAKAT.ConServices beschrieben.
- Die Benachrichtigung des Anschlussnutzers über die Parametrierung dieses TAF wird durch zu protokollierende Ereignisse in ▸FAKAT.ValProcConfig beschrieben.

3.3.7 TAF14: Hochfrequente Messwertbereitstellung für Mehrwertdienste

3.3.7.1 Beschreibung

Dieser Anwendungsfall erlaubt die hochfrequente Erfassung und Bereitstellung von Messwerten als Grundlage zur Umsetzung von Mehrwertdiensten (z.B. die Visualisierung der Messwerte für den Anschlussnutzer durch ein Internetportal). Die aktuellen Messwerte werden dem über das Auswertungsprofil zugeordneten Anschlussnutzer bzw. Anlagenbetreiber lokal bereitgestellt.

Berechtigte Empfänger sind grundsätzlich alle Marktteilnehmer (z.B. Lieferanten, Direktvermarkter und Aggregatoren), die über eine Einwilligung des Anschlussnutzers für die jeweilige Datenerhebung verfügen. Die Auswahl wird durch den GWA über das entsprechende Auswertungsprofil vorgegeben.

3.3.7.2 Anforderungen

Dieser TAF unterscheidet sich lediglich im Verwendungszweck und den zulässigen Messgrößen von anderen TAF aus ▸FAKAT.ValProcNonBilling. Da der technische Ablauf sonst identisch ist, wird an dieser Stelle stattdessen auf die relevanten Abschnitte verwiesen:

- Die Einschränkung der zulässigen Messgrößen für diesen TAF wird im Rahmen von Anforderungen an die Parametrierung in ▸FAKAT.ValProcConfig beschrieben.
- Der Empfang beziehungsweise Abruf von Messwerten der Messeinrichtung auf Basis der im Auswertungsprofil angegebenen Erfassungsperiode wird in ▸FAKAT.ValCapture beschrieben.
- Die Bildung und Zusammenfassung zu nicht-validierten Messwerten (siehe ▸NWL) für den Messwertversand wird in den generellen Anforderungen von ▸FAKAT.ValProcNonBilling beschrieben.
- Der Versand der nicht-validierten Messwerte wird in ▸FAKAT.ValTransmission beschrieben.
- Der lokale Abruf von Informationen zu diesem TAF für den Anschlussnutzer bzw. Anlagenbetreiber wird in ▸FAKAT.ConServices beschrieben.
- Die Benachrichtigung des Anschlussnutzers über die Parametrierung dieses TAF wird durch zu protokollierende Ereignisse in ▸FAKAT.ValProcConfig beschrieben.

3.4 Versand von Messwerten im WAN (FAKAT.ValTransmission)

3.4.1 Übersicht

Das SMGW übermittelt abrechnungsrelevante oder nicht-abrechnungsrelevante Messwerte periodisch oder im Bedarfsfall an den gemäß Auswertungsprofil berechtigten EMT. Die Übermittlung erfolgt authentisch und verschlüsselt an den EMT. Ein EMT-WAN-Kommunikationsprofil (siehe ▸FAKAT.EmtComConfig, parametriert durch den GWA) bestimmt die dabei zu verwendenden Kommunikationsparameter. Für die Gewährleistung der Nicht-Abstreitbarkeit der Herkunft der Messwerte können diese in Abhängigkeit der Parametrierung vom SMGW signiert werden.

Je nach Anwendungsfall und erhobenen Werten kann statt eines direkten Versands an den EMT ein Versand über den GWA notwendig sein, der die Werte an den EMT in verschlüsselter Form weiterleitet. Eine solche verschlüsselte Weiterleitung ist beispielsweise im Falle der Übermittlung pseudonymisierter Messwerte erforderlich.

3.4.2 Übersicht der FA

Aufgabe	Umsetzung
Auslieferung bilanzierungs- und abrechnungsrelevanter Messwerte an EMT	Das SMGW **MUSS** ▸FA.ExportAccntMtrReading umsetzen. [REQ.WAN.EmtBenachrichtigung.10]
Auslieferung nicht abrechnungsrelevanter Messwerte an EMT (z.B. Netzzustandsdaten)	Das SMGW **MUSS** ▸FA.ExportNonAccntMtrReading umsetzen. [REQ.WAN.EmtBenachrichtigung.20]

Aufgabe	Umsetzung
Auslieferung bilanzierungs- und abrechnungsrelevanter Messwerte via GWA an EMT	Das SMGW **SOLL** ▸FA.ExportAccntMtrReading "viaGwa" im Auswertungsprofil umsetzen (▸ICS.FAKAT.ValTransmission.10). [REQ.WAN.ZugriffAufGwaDienste.30]
Auslieferung nicht-zurechenbarer Messwerte via GWA an EMT	Das SMGW **SOLL** ▸FA.ExportNonAccntMtrReading "viaGwa" im Auswertungsprofil umsetzen. (▸ICS.FAKAT.ValTransmission.10). [REQ.WAN.ZugriffAufGwaDienste.40]
Versand im Bedarfsfall auslösen (bisher TAF6)	Das SMGW **MUSS** ▸FA.DoOnDemandDelivery für den GWA umsetzen. [REQ.FAKAT.MeteringConfig.80]
Versand (fehlender) historischer, registrierter Messwerte auslösen	Das SMGW **SOLL** ▸FA.DoReqExportHistoricReadings für den GWA umsetzen. (▸ICS.FAKAT.ValTransmission.10) [REQ.FAKAT.MeteringConfig.90]

Tabelle 3.13 Übersicht der FA der Kategorie FAKAT.ValTransmission

ICS



ICS.FAKAT.ValTransmission.10

Der GWH **MUSS** im ICS deklarieren, welche FAs das SMGW für den Export von Messwerten ins WAN umsetzt.

3.4.3 Datenstrukturen der FA-Kategorie

Die Datenstruktur für den Versand abrechnungsrelevanter registrierter Werte ist in ▸Abschnitt 3.22.35 beschrieben.

Die Datenstruktur für den Versand abrechnungsrelevanter abgeleiteter Werte ist in ▸Abschnitt 3.22.4 beschrieben.

Die Datenstruktur für den Versand nicht-abrechnungsrelevanter Messwerte ist in ▸Abschnitt 3.22.33 beschrieben.

Die Datenstruktur für den Export von Wertelisten und Logbüchern ist in ▸Abschnitt 3.22.17 beschrieben.

3.4.4 FA.ExportAccntMtrReading

3.4.4.1 Beschreibung

Das SMGW übermittelt auf Anforderung durch den GWA oder bei Erreichen des Versandauslösezeitpunktes die für den Versand gesammelten, für Abrechnungs- und Informationszwecke verwendbaren Messwerte einer Messeinrichtung an den EMT. Der Versandauslösezeitpunkt, die zu versendenden Messgrößen, die Identifikation des EMT und der Abrechnungsturnus werden einem vom GWA konfigurierten Auswertungsprofil entnommen. Nur die noch nicht zuvor an den EMT versandten Messwerte werden übermittelt.

Der Aufrufparameter bestimmt das Auswertungsprofil für den Versand.

Das SMGW erzeugt für den Versand von abrechnungsrelevanten Messwerten eine Datenstruktur, signiert sie gemäß Auswertungsprofil mit dem Signaturschlüssel des SMGW und initiiert die Nachrichtenübermittlung gemäß EMT-WAN-Kommunikationsprofil authentisch verschlüsselt für den EMT[4] an den WAN-Kommunikationspartner (EMT/GWA).

Das Ergebnis der Zustellung an den WAN-Kommunikationspartner wird protokolliert.

Der Inhalt des Messwertversands von ▸RWL bzw. ▸AWL enthält die Informationen aus ▸Tabelle 3.14 mit Verweis auf die relevanten Datenfelder.

Information	Datenfeld ▸RWL	Datenfeld ▸AWL
Identifikation der Messgrößen (OBIS)	▸columns.obis	▸values.obis
Messgeräteidentifikation	▸meterId	▸meterId

[4] Sowohl TLS für den direkten Transport zum EMT als auch CMS bei Auslieferung über den GWA ermöglichen die authentische Verschlüsselung.

Information	Datenfeld ▸RWL	Datenfeld ▸AWL
Zeitstempel	▸ts	▸ts
Messwert bzw. abgeleiteter Wert	▸values	▸values
Kombinierte Statuswort	▸combinedStatus	▸combinedStatus
Einheiten	▸columns.unit	▸values.unit
Typ des TAF	-	▸tafType

Tabelle 3.14 Übersicht der FA der Kategorie FAKAT.ClsServices

Weitere vom GWA im ▸Auswertungsprofil konfigurierte, aber nicht vom SMGW verarbeitete Informationen, wie die Anwendungsreferenz (▸tafId), können vorhanden sein. Zum Versand wird die ▸Exportstruktur verwendet.

Der Versand wird eingeschränkt auf den Gültigkeitszeitraum des Auswertungsprofiles, d.h. ein EMT erhält keine Messwerte, die vor dem Gültigkeitsbeginn oder nach dem Gültigkeitsende des Auswertungsprofiles von der Messeinrichtung empfangen und registriert wurden.

Durch den Parameter ▸meterDataOutput.viaGwa im ▸Auswertungsprofil kann der GWA veranlassen, dass die Messwerte - für den EMT gemäß EMT-WAN-Kommunikationsprofil verschlüsselt - mittels ▸WKS.ADMIN-SERVICE an den GWA zur Weiterleitung an den EMT übermittelt werden.

Die Struktur der exportierten Messwertliste (▸RWL , ▸AWL, jeweils mit/ohne Zeitreihe) richtet sich nach dem zugrundeliegenden TAF und dem Auslöser (periodischer Versand oder Anforderung im Bedarfsfall).

3.4.4.2 Auslöser

REQ.FA.ExportAccntMtrReading.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- (▸TAF1, ▸TAF2, ▸TAF7, ▸TAF8, ▸TAF15) Periodischer Versandauslösezeitpunkt gemäß Auswertungsprofil erreicht und noch nicht alle Werte im Abrechnungsturnus übermittelt.
- (▸TAF1, ▸TAF2, ▸TAF7, ▸TAF8) Anforderung durch GWA über ▸FA.DoOnDemandDelivery. ▸ [FNN.16004.0]
- (▸TAF1, ▸TAF2, ▸TAF7, ▸TAF8, ▸TAF15) Unmittelbar nach der ersten Messwertregistrierung nach Beginn des Gültigkeitszeitraumes eines Auswertungsprofiles (Erstauslesung).
- (▸TAF1, ▸TAF2, ▸TAF7, ▸TAF8, ▸TAF15) Unmittelbar nach letztem Sollregistrierzeitpunkt zum Ende des Gültigkeitszeitraumes eines Auswertungsprofiles (Schlussauslesung), wenn nicht bereits alle Werte im Abrechnungsturnus übermittelt wurden.

3.4.4.3 Anforderungen

Wird der TAF15 gemäß ▸ICS.FAKAT.ValProcBilling.20 nicht implementiert, kann kein Auswertungsprofil vom Typ TAF15 importiert werden. Aus diesem Grund sind die in den Anforderungen enthaltenen Prüfungen auf TAF15 dann nicht notwendig.

- (▸meterDataOutput.viaGwa="false") Das SMGW **MUSS** den Messwertversand über ▸WKS.INFO-REPORT mit den Transport- und Inhaltsdatenparametern des per ▸meterDataOutput.wanPeerRef im ▸Auswertungsprofil referenzierten WAN-Kommunikationsprofils durchführen. ▸ [BSI.16001.0] ▸ [BSI.16001.1] [REQ.FA.ExportAccntMtrReading.20]
- (▸meterDataOutput.viaGwa="true") Das SMGW **MUSS** den Messwertversand über ▸WKS.ADMIN-SERVICE mit den Transportparametern des GWA-WAN-Kommunikationsprofils "ADMIN-SERVICE" und den Inhaltsdatenverschlüsselungsparametern des per ▸meterDataOutput.wanPeerRef referenzierten EMT-WAN-Kommunikationsprofils durchführen (▸ICS.FAKAT.ValTransmission.10). ▸ [BSI.16001.0] ▸ [BSI.16001.1] [REQ.FA.ExportAccntMtrReading.25]
- (▸TAF1) Das SMGW **MUSS** den per ▸meterDataOutput.obis identifizierten Zählerstand als ▸Exportstruktur mit eingebetteter Datenstruktur ▸RWL übermitteln. [REQ.FA.ExportAccntMtrReading.30]

- (▸TAF1) Das SMGW **MUSS** den letzten zum Abrechnungszeitpunkt am Ende des Monats registrierten Zählerstand zum Versandauslösezeitpunkt oder Auslesezeitpunkt im Bedarfsfall übermitteln. [REQ.FA.ExportAccntMtrReading.40]
- (▸TAF1) Sofern zum Abrechnungszeitpunkt am Ende des Monats kein Zählerstand registriert wurde, **SOLL** das SMGW einen zeitähnlich gemäß ▸ICS.FA.ExportAccntMtrReading.10) registrierten Zählerstand zum Versandauslösezeitpunkt oder Auslesezeitpunkt im Bedarfsfall übermitteln. [REQ.FA.ExportAccntMtrReading.41]
- (▸TAF7) Das SMGW **MUSS** die per ▸meterDataOutput.obis im ▸Auswertungsprofil festgelegten, registrierten Zählerstände als ▸Exportstruktur mit eingebetteter Datenstruktur ▸RWL übermitteln. [REQ.FA.ExportAccntMtrReading.70]
- (▸TAF7, ▸TAF15) Das SMGW **MUSS** die letzten vor dem Versandauslösezeitpunkt gespeicherten Messwertdatensätze der per ▸meterReadingInput.meterId im ▸Auswertungsprofil identifizierten ▸RWL für den im ▸Auswertungsprofil angegebenen Zeitraum (▸taf7Params.billingInterval, ▸taf15Params.billingInterval) übermitteln. [REQ.FA.ExportAccntMtrReading.90]
- (▸TAF1, ▸TAF2, ▸TAF7, ▸TAF8, ▸TAF15) Das SMGW **MUSS** die Datenfelder der ▸Exportstruktur gemäß ▸Tabelle 3.15 setzen. [REQ.FA.ExportAccntMtrReading.100]
- (▸TAF2) Das SMGW **MUSS** den Zählerstand zum Ende des Abrechnungszeitraumes und die abgeleiteten Energiemengenregister (aller Tarifstufen und das Fehlerregister) zum Versandauslösezeitpunkt mit den Werten gemäß ▸meterDataOutput.obis übermitteln. [REQ.FA.ExportAccntMtrReading.120]
- (▸TAF8) Das SMGW **MUSS** den Zählerstand zum Ende des Abrechnungszeitraums, den abgeleiteten Lastgang für den im ▸Auswertungsprofil angegebenen Zeitraum (▸taf8Params.reportingPeriod) und den daraus gebildeten Maximumwert zum Versandzeitpunkt mit den Werten gemäß ▸meterDataOutput.obis übermitteln. [REQ.FA.ExportAccntMtrReading.130]
- (▸signMode<>"NONE") Das SMGW **MUSS** die kanonisierte ▸Exportstruktur mit dem Signaturverfahren ▸signMode gemäß ▸Auswertungsprofil und dem privaten Schlüssel GW_WAN_SIG_PRV bilden. [REQ.FA.ExportAccntMtrReading.110]
- (▸TAF2, ▸TAF7, ▸TAF8, ▸FA.DoReqExportHistoricReadings gemäß ▸ICS.FAKAT.ValTransmission.10 nicht implementiert) Das SMGW **MUSS** alle noch nicht versandten Werte versenden (die Einschränkung auf ▸taf7Params.billingInterval bzw. ▸taf8Params.reportingPeriod entfällt). [REQ.FA.ExportAccntMtrReading.140]
- Das SMGW **MUSS** gewährleisten, dass bei der Ausgabe von Messwerten nicht mehr Nachkommastellen als signifikante Stellen der Eingangsmessgrößen gemäß [DS] Kapitel SML bzw. [DS] Kapitel "wM-Bus" bezogen auf die Basiseinheit der Messgröße übermittelt werden. [REQ.FA.ExportAccntMtrReading.150] Eine Dezimalpunktverschiebung (z.B. Wh zu kWh) beeinflusst nicht die signifikanten Stellen, sofern die Einheit und Skalierungsfaktor erkennbar sind)

Datenfelder der ▸Exportstruktur	Ursprung
▸exportedData	▸TAF1, ▸TAF7, ▸TAF15: ▸RWL
	▸TAF2, ▸TAF8: ▸AWL
▸tafId	Anwendungsreferenz aus ▸tafId im ▸Auswertungsprofil.
▸gatewayId	Der SubjectCN des GW_WAN_TLS_CRT (entspricht dem SubjectCN des GW_WAN_SIG_CRT).
▸signature	Entfällt, sofern gemäß ▸signMode im ▸Auswertungsprofil keine Signatur erstellt wird.
▸signature.ts	Systemzeit des SMGW beim Aufruf (Signaturerstellungszeitpunkt).
▸signature.algo	Algorithmus gemäß ▸signMode im ▸Auswertungsprofil.
▸signature.originator	Die SMGW-ID (HÜID) des SubjectCN des GW_WAN_SIG_CRT.
▸signature.sigValue	Codierung und Wert basierend auf Verfahren gemäß ▸signMode im ▸Auswertungsprofil.

Tabelle 3.15 Übernahme von Datenfeldern in die exportierte Registrierte Werteliste

ICS



ICS.FA.ExportAccntMtrReading.10

Der GWH **MUSS** im ICS angeben (in Sekunden), in welchem Zeitbereich vor dem Abrechnungszeitpunkt am Monatsende zeitähnliche Zählerstände für TAF1 übermittelt werden können, wenn kein Zählerstand zum Abrechnungszeitpunkt registriert wurde. Der Wert 0 wird verwendet, wenn keine zeitähnlichen Zählerstände für TAF1 übermittelt werden. Ein Wert 3600 bedeutet, dass bis zu einer Stunde vor dem Abrechnungszeitpunkt registrierte Zählerstände übermittelt werden.

3.4.4.4 Implementierungshinweise

Der Versandauslösezeitpunkt ist der gemäß Auslösebedingungen vorgesehene Zeitpunkt, zu dem die ▸Exportstruktur erzeugt wird, nicht der Zeitpunkt der tatsächlichen Übermittlung an den EMT.

3.4.5 FA.ExportNonAccntMtrReading

3.4.5.1 Beschreibung

Das SMGW übermittelt auf Anforderung durch den GWA oder bei Erreichen des Versandzeitpunktes die für den Versand gesammelten, nicht für Abrechnungszwecke verwendbaren Messwerte einer Messeinrichtung an den EMT. Der Versandzeitpunkt, die zu versendenden Messgrößen, die Identifikation des EMT und der Zusammenfassungszeitraum werden einem vom GWA konfigurierten Auswertungsprofil entnommen. Nur die noch nicht zuvor an den EMT versandten Messwerte werden übermittelt.

Der (interne) Aufrufparameter bestimmt das Auswertungsprofil für den Versand.

Das SMGW erzeugt für den Versand eine Datenstruktur mit Messwerten und initiiert die Nachrichtenübermittlung gemäß EMT-WAN-Kommunikationsprofil authentisch verschlüsselt für den EMT[4] an den WAN-Kommunikationspartner (EMT/GWA).

Das Ergebnis der Zustellung an den WAN-Kommunikationspartner wird protokolliert. Im Fehlerfall wiederholt das SMGW die Zustellung wie im WAN-Kommunikationsprofil vorgegeben.

Der Inhalt der Messwertnachricht gemäß ▸NWL enthält mit Verweis auf die relevanten Datenfelder:

- die Identifikation der Messgrößen (OBIS, ▸meterId),
- die Messgeräteidentifikation (▸columns.obis),
- den Zeitstempel (▸ts),
- die Messwerte (▸values),
- Das kombinierte Statuswort (▸combinedStatus),
- die Einheiten (▸columns.unit) und
- den Typ des TAF (▸tafType).

Weitere vom GWA im ▸Auswertungsprofil konfigurierte, aber nicht vom SMGW verarbeitete Informationen, wie die Anwendungsreferenz (▸tafId), können vorhanden sein. Zum Versand wird die ▸Exportstruktur verwendet.

Je nach Verwendungszweck der Messwerte kann eine Pseudonymisierung erforderlich sein. Es ist die Aufgabe des GWA dies durch geeignete Konfiguration (▸meterDataOutput.viaGwa und ▸taf10Params.pseudonym im ▸Auswertungsprofil) sicherzustellen.

Netzwerkdiagnosedaten gemäß ▸FAKAT.NetworkDiagnosis fallen nicht unter die Netzzustandsdaten nach § 2 [MsbG]. Eine Pseudonymisierung beim Versand von Netzwerkdiagnosedaten ist daher nicht erforderlich.

Durch den Parameter ▸meterDataOutput.viaGwa im ▸Auswertungsprofil kann der GWA veranlassen, dass die Messwerte - für den EMT gemäß EMT-WAN-Kommunikationsprofil verschlüsselt - mittels WKS ADMIN-SERVICE an den GWA zur Weiterleitung an den EMT übermittelt werden.

▸Abbildung 3.7 zeigt das Auslösen des Messwertversands bei Über- oder Unterschreitung des Schwellwertes (incl. Hysterese) einer Messgröße. Die Parameter sind im Auswertungsprofil als ▸meterDataOutput.trigger.thresholds festgelegt. Mehrere Auslöser sind parametrierbar.

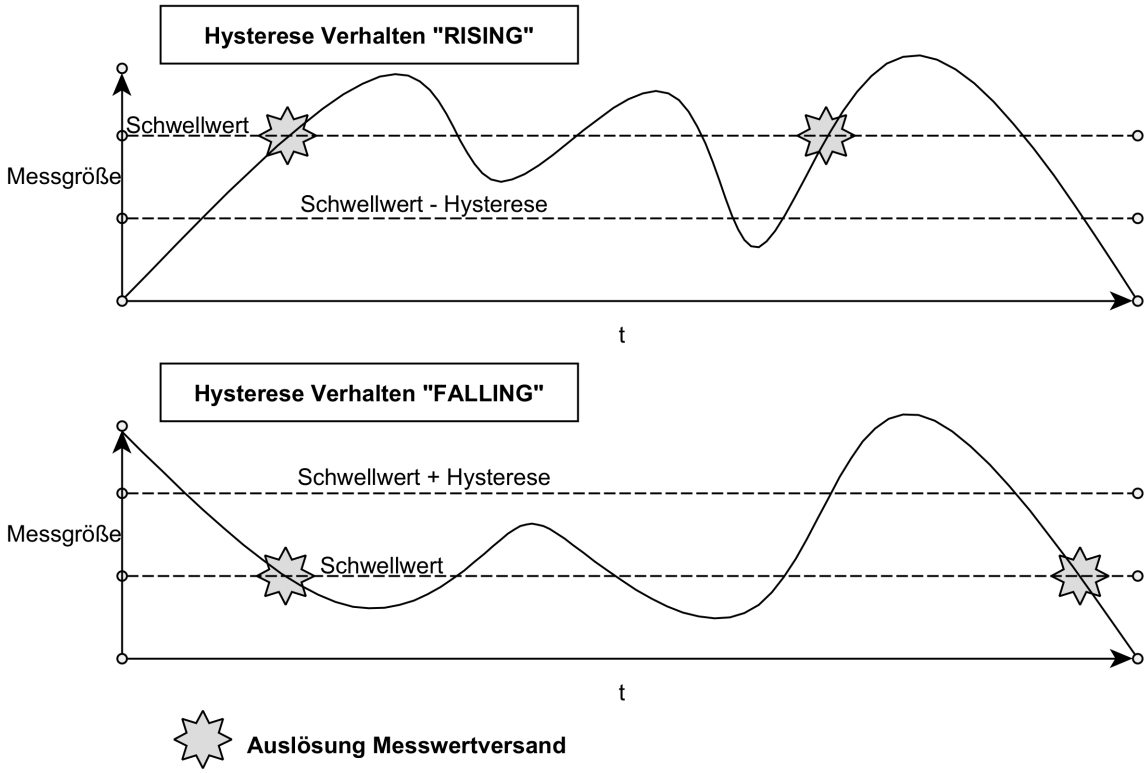


Abbildung 3.7. Verhalten bei Über- oder Unterschreitung von Schwellwerten mit Hysterese

Abbildung 3.8 zeigt den Ablauf für die Versandauslösebedingung des TAF9, TAF10, TAF14.

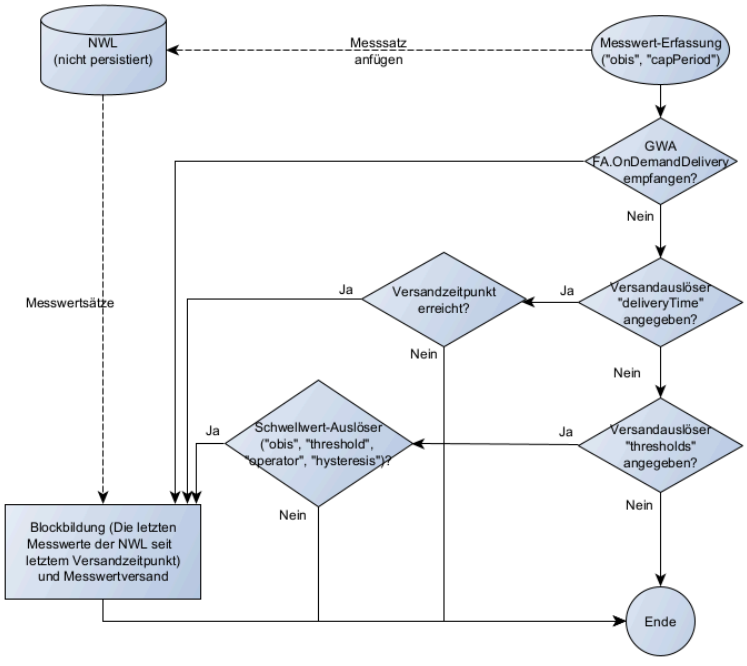


Abbildung 3.8. Ablauf der verschiedenen Versandauslösebedingungen

3.4.5.2 Auslöser

REQ.FA.ExportNonAccntMtrReading.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Periodischer Versandzeitpunkt gemäß Auswertungsprofil erreicht und noch nicht bereits alle Werte im seit dem letzten Versandzeitpunkt übermittelt.

- Versandanfrage durch GWA über ▸FA.DoOnDemandDelivery. ▸ [FNN.16004.0]
- Schwellwert gemäß Auswertungsprofil "Auslöser" unter- oder überschritten. ▸ [BSI.16008.0]
- Ad-hoc bei Empfang eines Messwerts, wenn gemäß Auswertungsprofil weder ein periodischer Versand noch ein Schwellwertversand parametriert ist.

3.4.5.3 Anforderungen

- Sofern ein Pseudonym für die Zähler-Identifikation im Auswertungsprofil vorhanden ist, **MUSS** das SMGW die Identifikation des Zählers in den versendeten Daten durch dieses Pseudonym ersetzen. [REQ.MWV.Pseudonymisierung.10]
- (▸meterDataOutput.viaGwa="false") Das SMGW **MUSS** den Messwertversand über ▸WKS.INFO-REPORT mit den Transport- und Inhaltsdatenparametern des per ▸meterDataOutput.wanPeerRef im ▸Auswertungsprofil referenzierten WAN-Kommunikationsprofils durchführen. ▸ [BSI.16001.0] ▸ [BSI.16001.1] ▸ [BSI.16007.1] ▸ [BSI.16008.1] [REQ.FA.ExportNonAccntMtrReading.20]
- (▸meterDataOutput.viaGwa="true") Das SMGW **MUSS** den Messwertversand über ▸WKS.ADMIN-SERVICE mit den Transportparametern des GWA-WAN-Kommunikationsprofils "ADMIN-SERVICE" und den EMT-WAN-Kommunikationsprofil Inhaltsdatenverschlüsselungsparametern des per ▸meterDataOutput.wanPeerRef referenzierten EMT-WAN-Kommunikationsprofils durchführen (▸ICS.FAKAT.ValTransmission.10). ▸ [BSI.16001.0] ▸ [BSI.16001.1] [REQ.FA.ExportNonAccntMtrReading.25]
- Das SMGW **MUSS** für ▸TAF9, ▸TAF10, ▸TAF14 die erfassten Messwerte gemäß ▸Exportstruktur für die Datenstruktur ▸NWL und den "zu Versendenden Werten" gemäß Auswertungsprofil übermitteln. [REQ.FA.ExportNonAccntMtrReading.30]
- Das SMGW **MUSS** für ▸TAF9, ▸TAF10, ▸TAF14 die erfassten Messwerte zum Versandzeitpunkt oder Auslesezeitpunkt im Bedarfsfall, eingeschränkt auf den Gültigkeitszeitraum des Auswertungsprofiles, übermitteln. [REQ.FA.ExportNonAccntMtrReading.40]
- Das SMGW **MUSS** die letzten vor dem Versandauslösezeitpunkt gespeicherten, noch nicht an den EMT versandten Messwertdatensätze der mit der ▸meterReadingInput.meterId des Auswertungsprofiles verknüpften ▸NWL übermitteln. [REQ.FA.ExportNonAccntMtrReading.50]
- Das SMGW **MUSS** die Datenfelder der ▸Exportstruktur und der exportierten ▸NWL gemäß ▸Tabelle 3.16 setzen. [REQ.FA.ExportNonAccntMtrReading.60]

Datenfeld ▸Exportstruktur	Ursprung
▸exportedData	▸TAF9, ▸TAF10, ▸TAF14: ▸NWL
▸tafId	Anwendungsreferenz aus dem gleichnamigen Datenfeld des mit der ▸meterReadingInput.meterId verknüpften Auswertungsprofiles, sofern der Parameter vorhanden ist.
▸signature	Entfällt, sofern gemäß Auswertungsprofil ▸signMode keine Signatur erstellt wird.
▸signature.ts	Systemzeit des SMGW beim Aufruf (Signaturerstellungszeitpunkt)
▸signature.algo	Gemäß Auswertungsprofil ▸signMode
▸signature.originator	Die SMGW-ID (HÜID) des SubjectCN des GW_WAN_SIG_CRT. Entfällt bei TAF10, wenn ▸taf10Params.pseudonym vorhanden ist.
▸signature.sigValue	Codierung und Wert gemäß des im Auswertungsprofil ▸signMode benannten Verfahrens

Tabelle 3.16 Übernahme von Datenfeldern beim Export

3.4.5.4 Implementierungshinweis

Die Ereignisse zum erfolgreichen Versand von Messwerten sollten in der Protokollierung - beispielsweise stündlich - zusammengefasst werden.

3.4.6 FA.DoOnDemandDelivery

3.4.6.1 Beschreibung

Dieser FA erlaubt den Versand von Messwerten im Bedarfsfall, ausgelöst durch den GWA. Die Auswahl des TAF und dem daraus für den Versand zu berücksichtigenden EMT sowie die zu versendenden Werte erfolgt durch Angabe des Auswertungsprofils im Rahmen eines Aufrufparameters (siehe ▸Parametersatz für die Auslesung im Bedarfsfall).

Der FA bildet die folgenden Fälle ab, in Abhängigkeit des TAF:

- Für ▸TAF1, ▸TAF7, ▸TAF8, ▸TAF15: Übermittlung eines tagesgenauen Zählerstandes zu einem konkreten Stichtag. Der Versand geschieht über ▸FA.ExportAccntMtrReading.
- Für ▸TAF2: Übermittlung eines tagesgenauen Standes der Energiemengenregister zu einem konkreten Stichtag. Der Versand geschieht über ▸FA.ExportAccntMtrReading.
- Für ▸TAF9, ▸TAF10, ▸TAF14: einmalige, sofortige Auslösung eines Versands aktueller Messwerte. Der Versand geschieht über ▸FA.ExportNonAccntMtrReading

Der Aufrufparameter lässt zusätzlich die Wahl eines Stichtags zu. Dies ist nur für TAF aus ▸FAKAT.ValProcBilling relevant und wird für TAF aus ▸FAKAT.ValProcNonBilling abgelehnt.

Das Vorhalten von tagesgenauen Mess- und Registerwerten für ▸TAF1, ▸TAF2, ▸TAF7, ▸TAF8 und ▸TAF15 für einen Zeitraum von 6 Wochen wird über diesen FA implizit für jeden konfigurierten TAF gefordert. Quelle für einen entsprechenden Wert kann abhängig vom TAF und seiner Parametrierung die ▸RWL, die ▸AWL oder eine unbenannte, SMGW-interne Messwertliste sein.

Der Versand findet unabhängig von einem historischem Versandstatus statt, da es aufgrund von technischen Fehlern beim EMT zum Datenverlust gekommen sein kann und eine erneute Übertragung notwendig sein kann.

3.4.6.2 Auslöser



REQ.FA.DoOnDemandDelivery.110

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.4.6.3 Anforderungen

- Das SMGW **MUSS** den Aufruf ablehnen, wenn der Aufrufparameter (▸profileId) kein zum Zeitpunkt der Auslesung gültiges (aktives) ▸Auswertungsprofil identifiziert. ▸ [BSI.16004.6] [REQ.FA.DoOnDemandDelivery.20]
- (▸TAF9, ▸TAF10 oder ▸TAF14) Das SMGW **MUSS** den Aufruf ablehnen, wenn der optionale Aufrufparameter (▸dueDate) gesetzt ist. ▸ [BSI.16004.8] [REQ.FA.DoOnDemandDelivery.80]
- (▸TAF1, ▸TAF2 ▸TAF7, ▸TAF8, ▸TAF15) Sofern kein Aufrufparameter ▸dueDate angegeben ist, **MUSS** das SMGW das Datum des Vortages der aktuellen Systemzeit für ▸dueDate verwenden. [REQ.FA.DoOnDemandDelivery.11]
- Das SMGW **MUSS** den Aufruf ablehnen, wenn der optionale Aufrufparameter (▸dueDate) mehr als 6 Wochen gegenüber der aktuellen Systemzeit in der Vergangenheit oder außerhalb des Gültigkeitszeitraums liegt. ▸ [BSI.16004.7] [REQ.FA.DoOnDemandDelivery.10]
- (▸TAF1) Das SMGW **MUSS** den im SMGW zum Sollregistrierzeitpunkt am Ende des Auslesetages gespeicherten Zählerstand und Status der Messgrößen übermitteln. [REQ.FA.DoOnDemandDelivery.30]
- (▸TAF7) Das SMGW **MUSS** den Registerstand und Status der Messgrößen zum letzten Sollregistrierzeitpunkt zum Ende des Tages der Bedarfsauslesung übermitteln. [REQ.FA.DoOnDemandDelivery.50]
- (▸TAF2) Das SMGW **MUSS** den Registerstand und Status der Messgrößen der abgeleiteten Werte (Registerstand aller Tarifstufenregister und des Fehlerregisters) zum letzten Sollregistrierzeitpunkt zum Ende des Tages der Bedarfsauslesung übermitteln. [REQ.FA.DoOnDemandDelivery.90]

- (▸TAF8) Das SMGW **MUSS** den Maximumwert und Zählerstand und Status der Messgrößen zum letzten Sollregistrierzeitpunkt zum Ende des Tages der Bedarfsauslesung übermitteln. [REQ.FA.DoOnDemandDelivery.100]
- (▸TAF9, ▸TAF10, ▸TAF14) Sofern die zugeordnete Messeinrichtung über bidirektionale Kommunikation angebunden ist, **MUSS** das SMGW den Abruf der aktuellen Messwerte von der Messeinrichtung auslösen und bis zu 10 Sekunden auf den Messwertempfang warten. [REQ.FA.DoOnDemandDelivery.55]
- (▸TAF9, ▸TAF10, ▸TAF14) Sofern die zugeordnete Messeinrichtung über unidirektionale Kommunikation angebunden ist, **MUSS+** das SMGW die zuletzt empfangenen Messwerte übermitteln. ▸ [FNN.16004.4] [REQ.FA.DoOnDemandDelivery.60]
- (▸TAF1, ▸TAF2 ▸TAF7, ▸TAF8, ▸TAF15) Das SMGW **MUSS** den Export von abrechnungsrelevanten Messwerten im Bedarfsfall mittels ▸Exportstruktur (siehe ▸FAKAT.ValTransmission) initiieren. ▸ [FNN.16004.4] [REQ.FA.DoOnDemandDelivery.70]
- (▸TAF9, ▸TAF10 oder ▸TAF14) Das SMGW **MUSS** den Export von nicht abrechnungsrelevanten Messwerten im Bedarfsfall mittels ▸Exportstruktur (siehe ▸FAKAT.ValTransmission) initiieren. ▸ [FNN.16004.4] [REQ.FA.DoOnDemandDelivery.120]



ICS.FA.DoOnDemandDelivery.10

Der GWH **MUSS** im ICS erklären, ob das SMGW den FA.DoOnDemandDelivery für TAF9/10/14 für mittels LKS2 angebundene Zähler unterstützt.

3.4.7 FA.DoReqExportHistoricReadings

3.4.7.1 Beschreibung

Dieser FA erlaubt den nachholenden Versand von historischen Zählerständen, die beispielsweise nicht innerhalb der über ▸outboundConnection.retryConfig definierten Wiederholungen an den berechtigten EMT übermittelt werden konnten.

Nachdem ein Messwertversand (▸FA.ExportAccntMtrReading) final fehlschlägt, versucht das SMGW keine weiteren Versandwiederholungen. Es ist dann Aufgabe des GWA, die noch nicht versandten Messwerte über diesen FA abzurufen.

Aufrufparameter bestimmen das ▸Auswertungsprofil und den in der Vergangenheit liegenden Zeitraum für den nachholenden Messwertversand.

Für ▸TAF1 werden die Tageswerte der ▸RWL, für ▸TAF7 und ▸TAF15 werden die in der ▸RWL gespeicherten, für ▸TAF2 und ▸TAF8 die in der ▸AWL gespeicherten Messwerte über ▸FA.ExportAccntMtrReading an den im ▸Auswertungsprofil bezeichneten EMT übermittelt.

3.4.7.2 Auslöser



REQ.FA.DoReqExportHistoricReadings.80

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.4.7.3 Anforderungen

Wird der ▸TAF15 gemäß ▸ICS.FAKAT.ValProcBilling.20 nicht implementiert, kann kein Auswertungsprofil dieses Typs importiert werden. Aus diesem Grund sind die in den Anforderungen enthaltenen Prüfungen auf TAF15 dann nicht notwendig.

- Das SMGW **MUSS** den Aufruf ablehnen, wenn der Berichtszeitraum für den nachholenden Abruf ▸reportingPeriod nicht innerhalb des Gültigkeitszeitraumes ▸validityPeriod des über den Aufrufparameter referenzierten Auswertungsprofiles liegt. ▸ [BSI.16004.6] [REQ.FA.DoReqExportHistoricReadings.10]
- Das SMGW **MUSS** den Aufruf ablehnen, wenn der über den Aufrufparameter ▸profileId identifizierte TAF nicht vom Typ ▸TAF1, ▸TAF2, ▸TAF7, ▸TAF8 oder ▸TAF15 ist. [REQ.FA.DoReqExportHistoricReadings.20]

- (▸tafType gleich ▸TAF15 und ▸ks gleich "LKS1") Das SMGW **MUSS** den Abruf der - in der RWL des SMGW nicht vorliegenden - registrierten Messwerte von der Messeinrichtung für den Zeitraum ▸reportingPeriod im Aufrufparameter auslösen und bis zu 20 Sekunden auf die vollständige Übermittlung der Messwerte von der Messeinrichtung warten. [REQ.FA.DoReqExportHistoricReadings.50]
- (▸tafType gleich ▸TAF7 oder ▸TAF15)Das SMGW **MUSS** den Export der Einträge der RWL für den Zeitraum ▸reportingPeriod im Aufrufparameter auslösen. [REQ.FA.DoReqExportHistoricReadings.40]
- (▸tafType gleich ▸TAF2 oder ▸TAF8) Das SMGW **MUSS** den Export der Einträge der ▸AWL für den Zeitraum ▸reportingPeriod im Aufrufparameter auslösen. [REQ.FA.DoReqExportHistoricReadings.70]
- (▸tafType gleich ▸TAF1) Das SMGW **MUSS** den Export der Zählerstände der RWL zum Monatsende für den Zeitraum ▸reportingPeriod im Aufrufparameter auslösen. [REQ.FA.DoReqExportHistoricReadings.90]

3.5 Erfassung von Messwerten (FAKAT.ValCapture)

3.5.1 Übersicht

Diese FA-Kategorie beschreibt die Erfassung von Messwerten durch das SMGW.

Dazu gehören die Entgegennahme, Erfassung, Zeitstempelung von authentisch und integer empfangenen Messwerten, sowie die Bewertung der Aktualität von empfangenen Messwerten und die Überführung in eine einheitliche Semantik für die Messwertverarbeitung.

Das SMGW unterstützt für unidirektionale Kommunikationstechnologien den Empfang periodisch übermittelter Messwertnachrichten und für bidirektionale Kommunikationstechnologien den Abruf und Empfang von Messwerten. Die nach dem Empfang zu verarbeitenden Messgrößen werden über ein ▸Auswertungsprofil festgelegt, das durch den GWA konfiguriert werden muss (siehe ▸FAKAT.ValProcConfig).

Voraussetzung für den Empfang und die Verarbeitung der Messwerte im SMGW ist die vorherige kommunikative Anbindung der Messeinrichtung an das SMGW über ein LMN-Kommunikationsprofil, das durch den GWA konfiguriert werden muss (siehe ▸FAKAT.LmnComConfig).

Für die Abrechnung im geschäftlichen Verkehr werden registrierte Messwerte verwendet. Bestimmt durch ein ▸Auswertungsprofil wird die Messwertregistrierung entweder im SMGW (Siehe ▸Abschnitt 3.2.4) oder in einer registrierenden Messeinrichtung durchgeführt.

3.5.2 Übersicht der FA

Aufgabe	Umsetzung
Erfassung abgerufener Messwerte (LAF1)	Das SMGW **MUSS** ▸FA.CaptureRequestedMtrData für die Messeinrichtung umsetzen. [REQ.LMN.Messwertempfang.20]
Erfassung unaufgefordert empfangener Messwerten (LAF2)	Das SMGW **MUSS** ▸FA.CaptureUnsolicitedRcvdMtrData für die Messeinrichtung umsetzen. [REQ.LMN.Messwertempfang.30]
Erfassung abgerufener Messwerte, die in der Messeinrichtung registriert wurden	Das SMGW **MUSS+** ▸FA.CaptureRegisteredValues für die Messeinrichtung umsetzen. [REQ.LMN.Messwertempfang.50]

Tabelle 3.17 Übersicht der FA der Kategorie FAKAT.ValCapture

3.5.3 Datenstrukturen

Die Datenstruktur der Eingangsmesswerte ist in ▸Abschnitt 3.22.5 beschrieben.

Das Auswertungsprofil ist in ▸Abschnitt 3.22.6 beschrieben.

Die Datenstruktur des Messgerätestatus ist in ▸Abschnitt 3.22.28 beschrieben.

Die Datenstruktur der nicht-validierten Werteliste ist in ▸Abschnitt 3.22.33 beschrieben.

3.5.4 Empfang von Messwerten

3.5.4.1 Einleitung

Dieser Abschnitt beschreibt die Anforderungen beim Empfang und der Bildung der ▸Eingangsmesswerte. Diese Anforderungen gelten für die abrechnungsrelevanten (registrierten) als auch die nicht-abrechnungsrelevanten Messwerte.

Eine Messwertnachricht kann Messwerte zu verschiedenen Messzeitpunkten enthalten. Das SMGW bestimmt aus Informationen in der Messwertnachricht die Aktualität der Messwerte.

Das SMGW fügt beim Empfang einen Empfangszeitstempel des Messwertes hinzu (▸receiveTs). Sofern die ▸Eingangsmesswerte bereits einen Zeitstempel der Messeinrichtung enthalten, wird dieser Zeitstempel für die weitere Messwertverarbeitung ergänzend geführt (▸measurementTs).

▸Abbildung 3.9 erläutert die Bedeutung der Pfeile, Linien und Elemente der folgenden Grafiken.

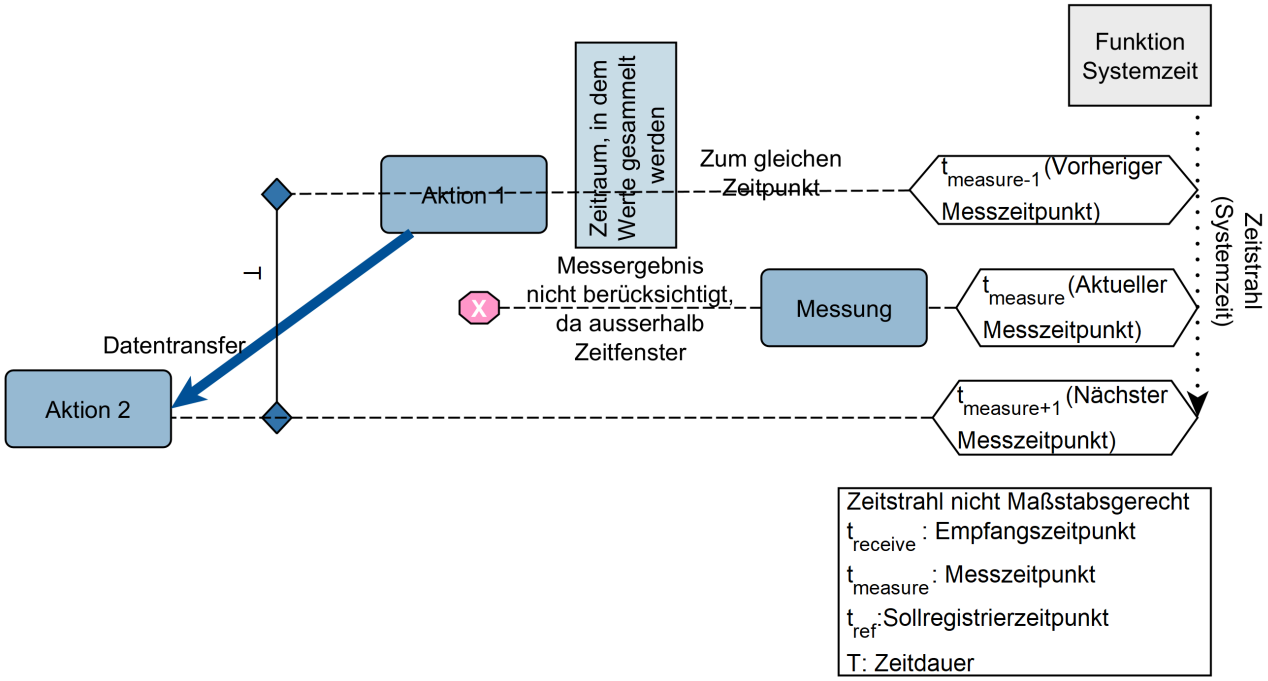


Abbildung 3.9. Legende und Zeichenerklärung für die folgenden Grafiken

3.5.4.2 Anforderungen

- Das SMGW **MUSS** das Datenfeld ▸receiveTs mit dem Empfangszeitpunkt der Messwertnachricht unter Verwendung der Systemzeit (Zeitskala UTC) des SMGW setzen. [REQ.FAKAT.ValCapture.10]
- Wenn die Messwertnachricht gemäß [DS] Informationen enthält, um die Latenz zwischen Messzeitpunkt und Versandzeitpunkt bestimmen zu können, **MUSS** das SMGW ▸ts gleich Empfangszeitpunkt (basierend auf der Systemzeit des SMGW) minus "Aktualitätsinformation" minus T_L ($T_{L,LKS1}$ gemäß ▸ICS.FA.CaptureRequestedMtrData.10, $T_{L,LKS2}$ gemäß ▸ICS.FA.CaptureUnsolicitedRcvdMtrData.10) setzen. [REQ.FAKAT.ValCapture.20]
- Sofern die Latenz zwischen Messzeitpunkt und Versandzeitpunkt nicht aus der Messwertnachricht bestimmt werden kann, **MUSS** das SMGW ▸ts gleich Empfangszeitpunkt (basierend auf der Systemzeit des SMGW) minus T_L. $T_{L,LKS1}$ gemäß ▸ICS.FA.CaptureRequestedMtrData.10, $T_{L,LKS2}$ gemäß ▸ICS.FA.CaptureUnsolicitedRcvdMtrData.20 setzen. [REQ.FAKAT.ValCapture.21]
- Das SMGW **MUSS** den ersten erfolgreichen Empfang einer Messwertnachricht (▸meter.pairingState gleich "DATA_EXCHANGE") nach Import oder Aktualisierung eines LMN-Kommunikationsprofils protokollieren. ▸ [FNN.1004.0] [REQ.FAKAT.ValCapture.30]

- Das SMGW **MUSS** nach Empfang der Messwertnachricht den kommunikativen Anbindungsstatus (mindestens ▸meter.pairingState, ▸meter.lastTs) der Messeinrichtung in der ▸Zählerstatusliste aktualisieren. [REQ.FAKAT.ValCapture.40]
- Sofern die empfangene Messwertnachricht für den Messwert einen absoluten Uhrzeitstempel der Messeinrichtung enthält, **MUSS** das SMGW diesen in der Zeitskala UTC mit Offset zur lokalen Zeitzone in das Datenfeld ▸measurementTs übernehmen. [REQ.FAKAT.ValCapture.50]

3.5.4.3 Statusinformationen

Die Bits des "Kombinierten Statuswortes" ▸combinedStatus gemäß [DS] Kapitel "Messwertstatus" werden aus dem jeweiligen Gerätestatus des SMGW und der zuliefernden Messeinrichtung (Siehe [DS] Kapitel "Wireless M-Bus Protokoll" und Kapitel "SML") gebildet. Sie lassen sich in folgende Kategorien einordnen:

Kategorie	Bedingung	Kombiniertes Statuswort
NO_ERROR (Fehlerfrei)	Dieser Wert wird verwendet, wenn die Messeinrichtung keinen Fehler zu dem Messwert mitsendet, die Integrität und Authentizität des Messwertes erfolgreich vom SMGW geprüft wurden und das SMGW selbst keinen abrechnungsrelevanten Fehler besitzt (wahrer Wert).	**SMGW_NoValue** = 0 und **MTR_Error** = 0 und **SMGW_Error** = 0 und **MTR_Fatal** = 0 und **SMGW_TimeNotValid** = 0 und **MTR_TimeNotValid** = 0
WARNING (Warnung)	Dieser Wert wird verwendet, wenn ein Fehlerstatus gesetzt ist, der jedoch keinen Einfluss auf die Gültigkeit des Messwertes hat (wahrer Wert). Im Rahmen der Messwertverarbeitung gilt ein solcher Messwert wie ein fehlerfreier Messwert. Der Status kann darauf hindeuten, dass künftig eine Aktion notwendig wird (z.B. geringer Batteriestand bei batteriebetriebenen Messeinrichtungen).	**MTR_Tamper** = 1 oder **MTR_Warning** = 1 oder **SMGW_Warning** = 1
MISSING_VALUE (Fehlender Wert)	Dieser Wert wird verwendet, wenn kein Wert eingetroffen ist, der innerhalb des Akzeptanzfensters liegt.	**SMGW_NoValue** = 1
TEMPORARY_ERROR (Gestörter Wert)	Es ist ein temporärer Fehler aufgetreten und der Messwert daher ungültig. Nach Behebung des Fehlers können zukünftige Messwerte wieder gültig sein.	**MTR_Error** = 1 oder **MTR_TimeNotValid**= 1 oder **SMGW_TimeNotValid** = 1
PERMANENT_ERROR (Dauerhafter Fehler)	Es ist ein fataler Fehler in der Messeinrichtung oder im SMGW aufgetreten. Der aktuelle und alle zukünftigen Messwerte sind ungültig.	**SMGW_Error** = 1 oder **MTR_Fatal** = 1

Tabelle 3.18 Statuskategorien der Messwerte im kombinierten SMGW-/Messgerätestatuswort in den Wertelisten

3.5.5 FA.CaptureRequestedMtrData

3.5.5.1 Beschreibung

Die über ▸meterReadingInput.meterId identifizierte Messeinrichtung verhält sich passiv und stellt erst dann einen Messwert zur Verfügung, wenn sie dazu vom SMGW aufgefordert wird. Das SMGW ruft die über OBIS-IDs im ▸Auswertungsprofil konfigurierten Messgrößen von der Messeinrichtung ab.

Dieser Anwendungsfall erfordert aufgrund des Request-/Response-Kommunikationsmusters eine bidirektionale Kommunikation mit der Messeinrichtung. Das SMGW erfasst ausschließlich authentisch und kryptografisch integer empfangene Nachrichten. Dabei gewährleistet die TLS-Verbindung (siehe ▸LKS1) eine kryptografische Integrität, die auf dem Transportweg zwischen Messeinrichtung und SMGW ausgelassene, duplizierte, vertauschte oder veränderte Nachrichten verhindert. Die Authentizität gewährleistet eine Nicht-Abstreitbarkeit der Herkunft der Nachricht aus der Messeinrichtung, die im Besitz der kryptografischen Identität (des geheimen Schlüssels) ist.

Ein ▸Auswertungsprofil bestimmt den Abruf von Messwerten aus der Messeinrichtung (▸meterReadingInput.meterId), die abzurufenden Messgrößen (▸meterReadingInput.obis), den Takt der Messwertabfrage (Registrierperiode für abrechnungsrelevante und Erfassungsperiode für nicht-abrechnungsrelevante Messwerterfassung) und die Zeitstempelungsmethode für die Weiterverarbeitung der Messwerte.

Das SMGW setzt die protokollspezifische Repräsentation von Messwert, Messgerätestatus, Identifikation von Einheit und Messgröße, Skalierungsfaktor und optionalem Messzeitpunkt für die Messwertverarbeitung in eine einheitliche Semantik um (siehe ▸Eingangsmesswerte).

Dieser FA ist nicht für den nachholenden Abruf historischer Messwerte aus registrierenden Messeinrichtungen zu verwenden.

▸Abbildung 3.10 zeigt den zeitlichen Zusammenhang von Messung, LMN-Kommunikation und Empfang im SMGW, wobei der Messwertversand aus der Messeinrichtung über eine bidirektionale Kommunikation durch das SMGW ausgelöst wird.

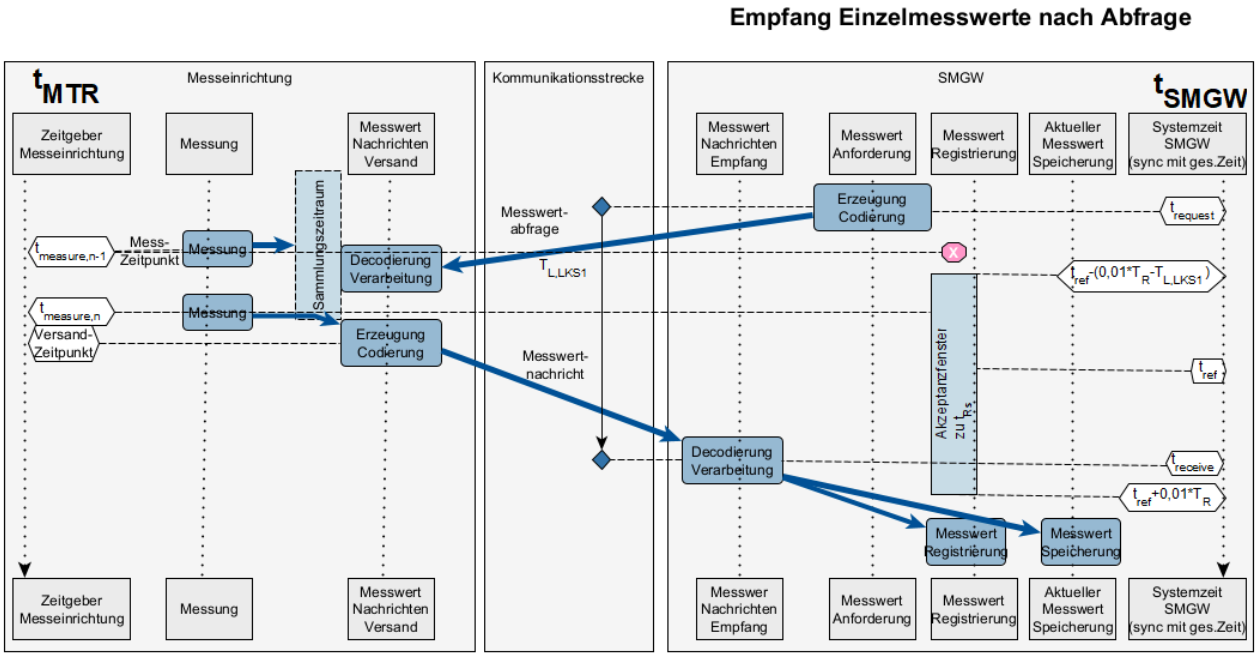


Abbildung 3.10. Zeitlicher Zusammenhang von Messung, Abfrage und Erfassung über LKS1

3.5.5.2 Auslöser

REQ.FA.CaptureRequestedMtrData.10

Das SMGW **MUSS** den FA.CaptureRequestedMtrData bei den in ▸Tabelle 3.19 genannten Ereignissen und Zeitpunkten auslösen.

Ereignis	Zugrundeliegende Parametrierung
Systemzeit überschreitet die Vorlaufzeit vor einem Sollregistrierzeitpunkt gemäß ▸ICS.FA.CaptureRequestedMtrData.10	Jedes aktive Auswertungsprofil für ▸TAF1, ▸TAF2, ▸TAF7 und ▸TAF8, bei dem das per ▸meterReadingInput.meterId verknüpfte LMN-Kommunikationsprofil ein LKS für bidirektionale Kommunikation parametriert hat. Das Auswertungsprofil definiert über den Parameter ▸taf1Params.regInterval, ▸taf2Params.regInterval, ▸taf7Params.regInterval, ▸taf8Params.regInterval die Sollregistrierzeitpunkte.
Systemzeit überschreitet einen Empfangszeitpunkt.	Jedes aktive Auswertungsprofil für ▸TAF9, ▸TAF10 oder ▸TAF14, bei dem das per ▸meterReadingInput.meterId verknüpfte LMN-Kommunikationsprofil ein bidirektionales LKS parametriert hat. Das Auswertungsprofil definiert über ▸taf9Params.capPeriod, ▸taf10Params.capPeriod bzw. ▸taf14Params.capPeriod die Empfangszeitpunkte.
Abruf aktueller Messwerte ausgelöst durch den Aufruf von ▸FA.ReadInstantMtrReading	Jedes aktive Auswertungsprofil, dessen Parameter ▸meterReadingInput.meterId dem Aufrufparameter von ▸FA.ReadInstantMtrReading entspricht.

Ereignis	Zugrundeliegende Parametrierung
Abruf aktueller Messwerte ausgelöst durch den Aufruf von ▸FA.DoOnDemandDelivery	Jedes aktive Auswertungsprofil für ▸TAF9, ▸TAF10 oder ▸TAF14 dessen Parameter ▸meterReadingInput.meterId dem Aufrufparameter von ▸FA.ReadInstantMtrReading entspricht.

Tabelle 3.19 Auslöser für Messwertabfrage

3.5.5.3 Anforderungen

- Das SMGW **MUSS** die Messwertabfrage nicht durchführen, sofern ▸active des zugeordneten LMN-Kommunikationsprofils "false" ist. [REQ.FA.CaptureRequestedMtrData.80]
- Das SMGW **MUSS** eine Messwertanforderung an die über ▸meterReadingInput.meterId im Auswertungsprofil identifizierte Messeinrichtung senden und dabei das im LMN-Kommunikationsprofil angegebene bidirektionale LKS verwenden. [REQ.FA.CaptureRequestedMtrData.20]
- Das SMGW **MUSS** nach Auslösen des FA die über ▸meterReadingInput.obis identifizierten Messgrößen und Messwert- und Messgerätestatusinformationen aller mit der ▸meterReadingInput.meterId verknüpften Auswertungsprofile anfordern. [REQ.FA.CaptureRequestedMtrData.30]
- Sofern die Messwertnachricht über ▸LKS1 empfangen wurde, **MUSS** das SMGW die Messwertnachricht gemäß [DS] Kapitel "SML" (Identifikation der Messgrößen, Konvertierung der Wertebereiche, Messgeräte- und Messwertstatus, Zeitliche Anforderungen) mit der Bedeutung der Datenfelder gemäß ▸Eingangsmesswerte und Statusinformationen gemäß ▸Messgerätestatus für die Messwertverarbeitung bereitstellen. [REQ.FA.CaptureRequestedMtrData.40]
- Nach Empfang einer Messwertnachricht **MUSS** das SMGW die Anforderungen aus ▸Abschnitt 3.5.4.2 umsetzen, um daraus eine einheitliche Struktur (▸Eingangsmesswerte) zu bilden. [REQ.FA.CaptureRequestedMtrData.51]
- Das SMGW **MUSS** die Messwertanfrage mit der Häufigkeit ▸ICS.FA.CreateProcessingProfile.30 wiederholen können. [REQ.FA.CaptureRequestedMtrData.75]

ICS



ICS.FA.CaptureRequestedMtrData.10

Der GWH **MUSS** im ICS die maximale angenommene Latenz ($T_{L,LKS1}$) zwischen Versand der Abfrage an die Messeinrichtung und Empfangszeitstempelung der Antwort im SMGW für die Kommunikation über LKS1 angeben (max. 4 Sekunden). Diese Latenz setzt sich zusammen aus der Kommunikationslatenz und der Verarbeitungslatenz der Messeinrichtung. Sofern sie dem GWH nicht bekannt ist, soll der Wert 4 Sekunden angegeben werden.

3.5.5.4 Implementierungshinweis

Das SMGW kann Abfragen zu verschiedenen Auslösern zusammenfassen, sofern die Anforderungen verschiedener Auswertungsprofile eingehalten werden.

Die Implementierung kann im Falle von Übertragungsstörungen, die zum Verlust von Nachrichten führen (Anfrage an die Messeinrichtung oder Antwort von der Messeinrichtung) und durch einen Timeout erkannt werden, auf Transportebene Nachrichten wiederholen, um einen zuverlässigen Transport zu gewährleisten, solange sich diese im Akzeptanzfenster für den Sollregistrierzeitpunkt bzw. 2 Sekunden (jeweils der kleinste Wert) nicht überschreiten.

3.5.6 FA.CaptureUnsolicitedRcvdMtrData

3.5.6.1 Beschreibung

Das SMGW empfängt von Messeinrichtungen, unaufgefordert zugelieferte Messwertnachrichten. Das SMGW berücksichtigt für die Messwertverarbeitung nur die Messgrößen, die über OBIS-IDs im ▸Auswertungsprofil konfiguriert sind. Sofern im LMN-Kommunikationsprofil der Messeinrichtung der Parameter ▸active gleich "true" ist.

Das SMGW erfasst ausschließlich authentisch und kryptografisch integer empfangene Nachrichten. Dabei gewährleistet das auf einem gemeinsamen geheimen Schlüssel basierende IT-Sicherheitsprotokoll (siehe ▸LKS2) eine kryptografische Integrität, die auf dem Transportweg zwischen Messeinrichtung und SMGW ausgelassene, duplizierte, vertauschte oder veränderte Nachrichten verhindert. Die Authentizität gewährleistet eine Nicht-Abstreitbarkeit der Herkunft der Nachricht aus der Messeinrichtung, die im Besitz der kryptografischen Identität (des geheimen Schlüssels) ist.

Die authentisch empfangene Identifikation der Messeinrichtung und das LKS für unidirektionale Kommunikation bestimmt das aktive Auswertungsprofil, aus dem die zu verarbeitenden Messgrößen (▸meterReadingInput.obis) und die für die Registrierung von Messgrößen (siehe ▸Abschnitt 3.2.4) relevanten Parameter bestimmt werden.

Das SMGW setzt die protokollspezifische Repräsentation von Messwert, Messgerätestatus, Identifikation von Einheit und Messgröße, Skalierungsfaktor und optionalem Messzeitpunkt für die Messwertverarbeitung in eine einheitliche Semantik um (siehe ▸Eingangsmesswerte).

▸Abbildung 3.11 zeigt den zeitlichen Zusammenhang von Messung, LMN-Kommunikation und Empfang im SMGW, wobei der Messwertversand aktueller Messwerte periodisch, selbstständig durch die Messeinrichtung ausgelöst wird.

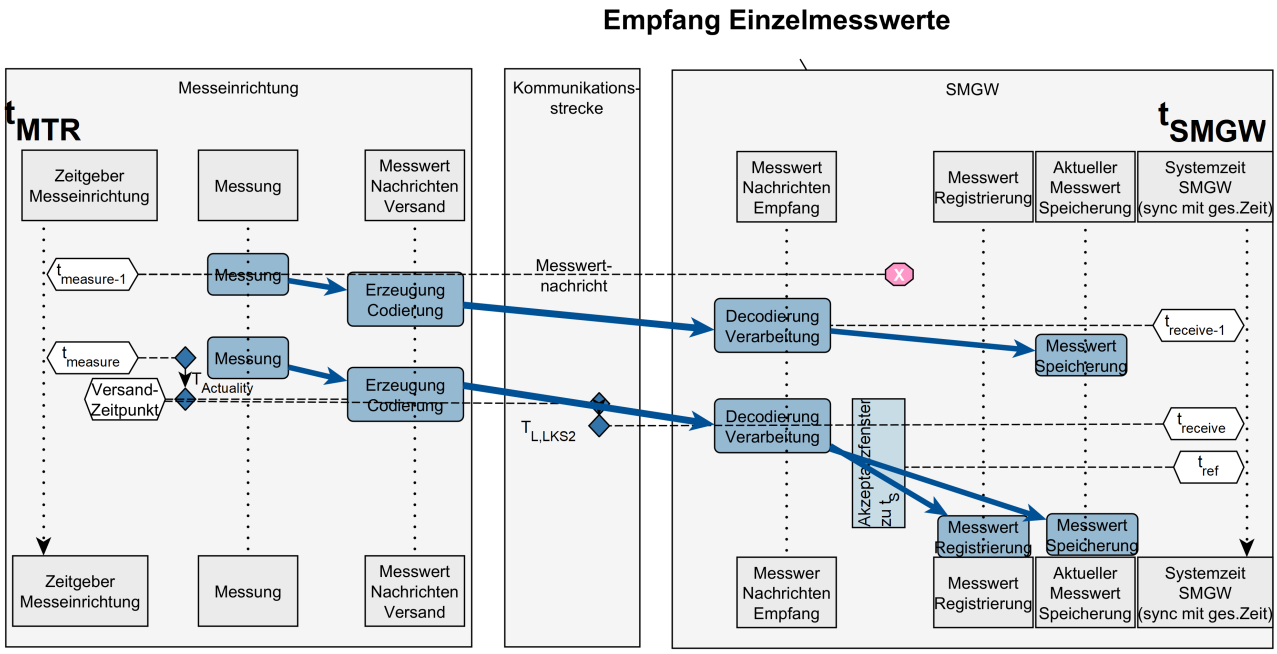


Abbildung 3.11. Zeitlicher Zusammenhang von Messung und Erfassung von Einzelwerten über LKS2

▸Abbildung 3.12 zeigt den zeitlichen Zusammenhang von Messung, LMN-Kommunikation und Empfang im SMGW für die gebündelte Übertragung der letzten Messwerte. Der Messwertversand wird periodisch, selbstständig durch die Messeinrichtung ausgelöst.

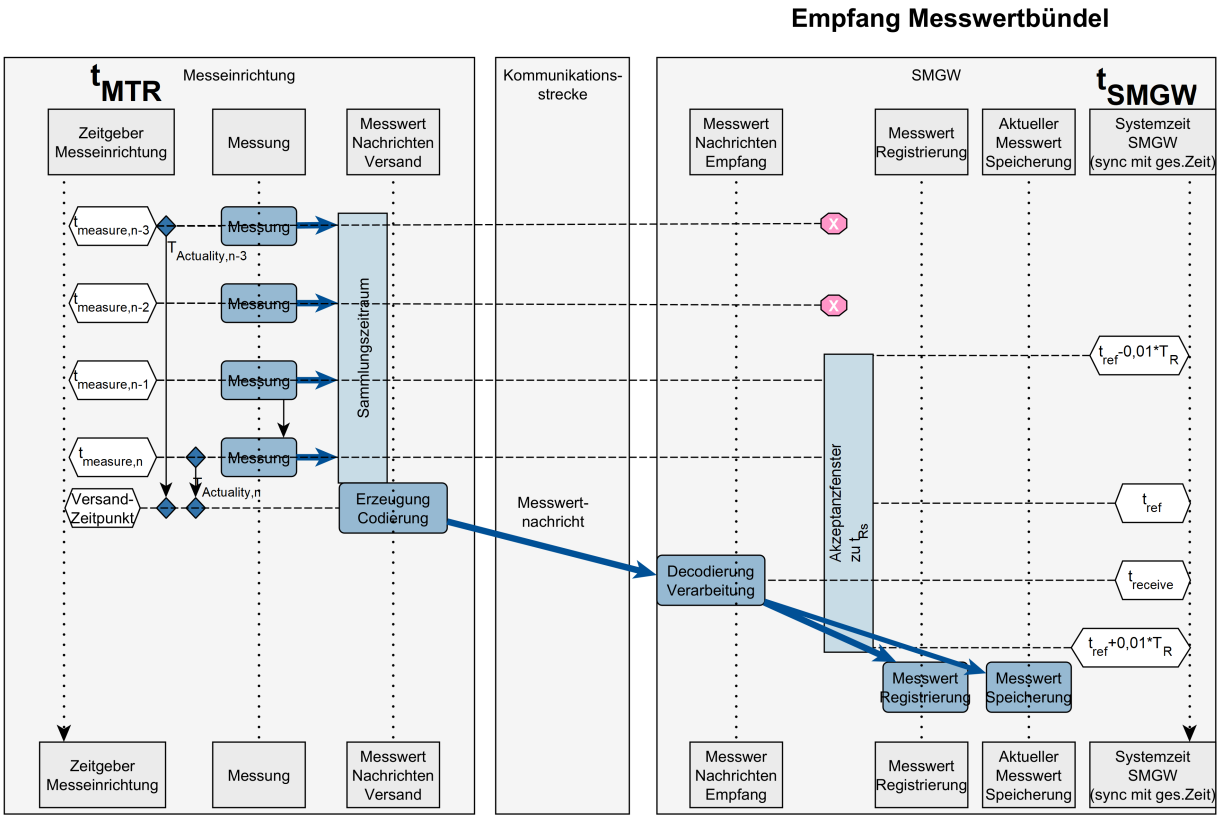


Abbildung 3.12. Zeitlicher Zusammenhang von Messung, Bündelversand und Erfassung über LKS2

3.5.6.2 Auslöser

REQ.FA.CaptureUnsolicitedRcvdMtrData.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Nachricht über ▸LKS2.

3.5.6.3 Anforderungen

- Das SMGW **MUSS** die Nachricht ignorieren (nicht verarbeiten), sofern ▸active des zugeordneten LMN-Kommunikationsprofils "false" ist. [REQ.FA.CaptureUnsolicitedRcvdMtrData.40]
- Das SMGW **MUSS** die Messwertnachricht gemäß [DS] Kapitel "wM-BUS" (Identifikation der Messgrößen, Konvertierung der Wertebereiche, Messgeräte- und Messwertstatus, zeitliche Anforderungen) mit der Bedeutung der Datenfelder der ▸Eingangsmesswerte und Statusinformationen (▸Messgerätestatus für die Messwertverarbeitung bereitstellen. [REQ.FA.CaptureUnsolicitedRcvdMtrData.20]
- Nach Empfang einer Messwertnachricht **MUSS** das SMGW die Anforderungen aus ▸Abschnitt 3.5.4.2 für jeden in der Messwertnachricht enthaltenen Messzeitpunkt umsetzen, um daraus eine einheitliche Struktur (▸Eingangsmesswerte) zu bilden. [REQ.FA.CaptureUnsolictedRcvdMtrData.31]

ICS

ICS.FA.CaptureUnsolicitedRcvdMtrData.10

Der GWH **MUSS** im ICS die maximale Latenz ($T_{L,LKS2}$) zwischen Messwertversand aus der Messeinrichtung und Empfangszeitstempelung im SMGW für die Kommunikation über LKS2 angeben (max. 4 Sekunden). Sofern nicht bekannt, wird die Latenz mit 4 Sekunden angenommen.

ICS.FA.CaptureUnsolicitedRcvdMtrData.20

Der GWH **MUSS** im ICS die maximale angenommene Latenz zwischen Messwertbildung und Empfangszeitstempelung im SMGW für die Kommunikation über LKS2 angeben (max. 4 Sekunden). Sofern nicht bekannt, wird die Latenz mit 4 Sekunden angenommen.

3.5.7 FA.CaptureRegisteredValues

3.5.7.1 Beschreibung

Das SMGW fragt für einen bestimmten Zeitraum von der im Aufrufparameter über das Auswertungsprofil identifizierten Messeinrichtung die mit Zeitstempeln versehenen Messwertsätze an, sofern ▸active "true" ist. Von der Messeinrichtung empfangene registrierte Messwerte werden in der zugeordneten Registrierten Messwertliste (RWL) des SMGW ergänzt, sofern sie nicht mit gleichem Messzeitpunkt und Identifikation der Messgröße bereits in der RWL vorliegen.

Der GWA/MSB sorgt dafür, dass die Registrierperiode der Messeinrichtung (▸measurementTs) mit der im Auswertungsprofil konfigurierten Registrierperiode (▸taf15Params.regInterval) übereinstimmt, indem er die bestellte/gelieferte Zählerkonfiguration der Registrierzeitpunkte prüft. Das SMGW übernimmt den von der Messeinrichtung bestimmten Zeitstempel ▸measurementTs in die RWL ▸ts und ergänzt den entsprechenden Sollregistrierzeitpunkt ▸refTs.

Der Anwendungsfall wird gemäß Auswertungsprofil periodisch oder im Bedarfsfall über ▸FA.DoReqExportHistoricReadings vom GWA initiiert.

Das SMGW gewährleistet die authentische und vertrauliche Übermittlung von der Messeinrichtung, die Integritätsgesicherte Speicherung in der RWL des SMGW und über ▸FA.ExportAccntMtrReading den authentischen und vertraulichen Versand an den berechtigen EMT.

Dieser Anwendungsfall erfordert eine bidirektionale Verbindung zwischen Zähler und SMGW.

Über das Auswertungsprofil ▸meterDataOutput.obis wird bestimmt, welche über OBIS-IDs identifizierten Registrierten Zählerstandsgänge oder Lastgänge abgerufen werden.

Die von der Messeinrichtung registrierten Messwerte werden im SMGW mit der OBIS-Kanalnummer B=0 registriert (Siehe ▸Abschnitt 2.5.2).

3.5.7.2 Auslöser



REQ.FA.CaptureRegisteredValues.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Die Systemzeit überschreitet 3 % der Registrierperiode gemäß ▸taf15Params.regInterval des letzten Sollregistrierzeitpunktes im Abrechnungsturnus ▸taf15Params.billingInterval.
- Anforderung durch den GWA über ▸FA.DoReqExportHistoricReadings, sofern in der Registrierten Werteliste für den Abfragezeitraum Zählerstände fehlen.
- Anforderung durch den Anschlussnutzer über ▸FA.ExportRegMtrReading, sofern in der Registrierten Werteliste für den Abfragezeitraum Zählerstände fehlen.
- Anforderung durch den Anschlussnutzer über ▸FA.ExportDailyMtrReading, sofern in der Tageswerteliste für den Abfragezeitraum Zählerstände fehlen.
- Anforderung durch den Anschlussnutzer über ▸FA.ExportDerivedMtrReading, sofern in der abgeleiteten Werteliste für den Abfragezeitraum Lastgangwerte fehlen.

3.5.7.3 Anforderungen

Die Umsetzung der folgenden Anforderungen ist abhängig von ▸ICS.FAKAT.ValProcBilling.20.

- Das SMGW **MUSS** die Messwertabfrage nicht durchführen, sofern ▸active des zugeordneten LMN-Kommunikationsprofils "false" ist. [REQ.FA.CaptureRegisteredValues.40]
- Falls der Aufruf periodisch durch das TAF15 Auswertungsprofil erfolgt, **MUSS** das SMGW den Abfragezeitraum vom Beginn bis zum Ende des gerade beendeten Abrechnungsturnus ▸taf15Params.billingInterval übermitteln und die Identifikation der Messgrößen des Auswertungsprofiles ▸meterReadingInput.obis gemäß [DS] Kapitel "SML" über ▸LKS1 zur Abfrage an die über ▸meterReadingInput.meterId identifizierte Messeinrichtung übermitteln. [REQ.FA.CaptureRegisteredValues.16]
- Falls der Aufruf über ▸FA.DoReqExportHistoricReadings für ein TAF15 Auswertungsprofil erfolgt, **MUSS** das SMGW die im Berichtszeitraum (▸reportingPeriod) in der RWL fehlenden Registrierzeitpunkte und

die Identifikation der Messgrößen des Auswertungsprofiles ▸meterReadingInput.obis gemäß [DS] Kapitel "SML" über ▸LKS1 zur Abfrage an die über ▸meterReadingInput.meterId identifizierte Messeinrichtung übermitteln. [REQ.FA.CaptureRegisteredValues.20]

- Das SMGW **MUSS** die von der Messeinrichtung über ▸LKS1 gemäß ▸Datenfelder des Datenobjekts "Eingangsmesswerte" (acquisitionData) empfangenen Datensätze in die der Messeinrichtung zugeordnete RWL einordnen, so dass in der RWL nur jeweils ein Messwertsatz pro Registrierzeitpunkt vorhanden ist und die Datensätze in chronologischer Reihenfolge exportiert werden können. Dabei dürfen bereits im SMGW vorliegende RWL-Einträge zum gleichen Registrierzeitpunkt nicht geändert werden. [REQ.FA.CaptureRegisteredValues.30]

3.5.7.4 Implementierungshinweise

Der Abruf der in der RWL fehlenden Werte kann entweder selektiv und mit Mehrfachabfrage für die fehlenden Registrierzeitpunkte oder in einer Abfrage mit Ignorieren doppelt empfangener Messwertsätze geschehen.

3.6 Dienste für lokale Nutzer (FAKAT.ConServices)

3.6.1 Übersicht

Das SMGW bietet eine Schnittstelle im HAN an, über die das SMGW dem berechtigten lokalen Nutzer (beispielsweise Anschlussnutzer, Anlagenbetreiber) seine Messwerte und andere für ihn relevante Informationen bereitstellt, um sie beispielsweise über einen Web-Browser zur Verbrauchsinformation oder Rechnungsprüfung zu visualisieren oder für sein Energiemanagement zu verwenden. Als Anzeigeeinheit kann zur Rechnungsprüfung ein Gerät mit Transparenz- und Display-Software nach [MessEG]/[MessEV] verwendet werden.

Unter Verwendung der Anwendungsfälle dieser FA-Kategorie kann somit die Bereitstellung von abrechnungsrelevanten Daten und von *aktuellen Werten* sowie die zugehörigen Tarifinformationen gemäß den Anwendungsfällen der Tarifierung aus ▸FAKAT.ValProcBilling gewährleistet werden. Ebenso ermöglicht der Anwendungsfall ▸FA.ExportDailyMtrReading die Bereitstellung von historischen Energieverbrauchs- oder Einspeisedaten. Werte werden unter Berücksichtigung der Vorhaltefristen bereitgestellt (siehe ▸Abschnitt 5.5).

Zusätzlich wird über ▸FA.ExportUserLog die Bereitstellung der Daten aus dem Anschlussnutzer-Log gewährleistet.

Den Anwendungsfällen dieser Kategorie ist gemein, dass das SMGW zur Ausführung des Anwendungsfalles einen Dienst für den Anschlussnutzer bereitstellt und eine entsprechende Antwort (bei erfolgreicher Ausführung oder auch im Fehlerfall) liefert.

Zu beachten ist, dass einem SMGW mehrere Anschlussnutzer zugeordnet sein können. Ein Anschlussnutzer darf nur auf die Daten zugreifen können, für die er autorisiert ist. Insbesondere muss ein unautorisierter Zugriff auf die Daten anderer Anschlussnutzer verhindert werden. Wird innerhalb dieser FA-Kategorie von *einem* oder *dem* Anschlussnutzer gesprochen, ist immer derselbe, identifizierte und authentifizierte Anschlussnutzer gemeint.

3.6.2 Übersicht der FA

Aufgabe	Umsetzung
Bereitstellung des dem Anschlussnutzer zugeordneten Logs	Das SMGW **MUSS** ▸FA.ExportUserLog für den Anschlussnutzer umsetzen [REQ.HAN.AnschlussnutzerDatenbereitstellung.10]
Auflistung der dem Anschlussnutzer zugeordneten FAs und Ressourcen	Das SMGW **MUSS+** ▸FA.ListSmgwResources für den Anschlussnutzer umsetzen.(▸ICS.FAKAT.ConServices.10) [REQ.HAN.AnschlussnutzerDatenbereitstellung.120]
Bereitstellung von Geräte Software- und Hardwareinformationen	Das SMGW **MUSS** ▸FA.ReadDeviceInfo für den Anschlussnutzer umsetzen [REQ.HAN.AnschlussnutzerDatenbereitstellung.30]
Bereitstellung der letzten empfangenen Messwerte der dem Anschlussnutzer zugeordneten Zähler	Das SMGW **MUSS** ▸FA.ReadInstantMtrReading für den Anschlussnutzer umsetzen. [REQ.HAN.AnschlussnutzerDatenbereitstellung.50]

Aufgabe	Umsetzung
Bereitstellung der historischen registrierten Messwerten der dem Anschlussnutzer zugeordneten Zähler (RWL)	Das SMGW **MUSS** ▸FA.ExportRegMtrReading für den Anschlussnutzer umsetzen [REQ.HAN.AnschlussnutzerDatenbereitstellung.40]
Bereitstellung der dem Anschlussnutzer zugeordneten historischen Tageszählerständen (TWL)	Das SMGW **MUSS** ▸FA.ExportDailyMtrReading für den Anschlussnutzer umsetzen. [REQ.HAN.AnschlussnutzerDatenbereitstellung.70]
Bereitstellung der dem Anschlussnutzer zugeordneten Auswertungsprofile und ihrer Tarif-Regelwerkparameter	Das SMGW **MUSS** ▸FA.ReadProcessingProfile (siehe ▸FAKAT.ValProcConfig) für den Anschlussnutzer umsetzen. [REQ.FAKAT.ConServices.20]
Bereitstellung der dem Anschlussnutzer zugeordneten abgeleiteten Werte (AWL)	Das SMGW **MUSS** ▸FA.ExportDerivedMtrReading für den Anschlussnutzer umsetzen. [REQ.FAKAT.ConServices.70]
Bereitstellung der dem Anschlussnutzer zugeordneten aktuellen Tarifinformationen und -stufen	Das SMGW **MUSS** ▸FA.ReadTariffState für den Anschlussnutzer umsetzen. [REQ.FAKAT.ConServices.80]
Bereitstellung des Zeitsynchronisations-Status des SMGW und der Lokalzeit.	Das SMGW **MUSS** ▸FA.ReadTimeSyncStatus für den Anschlussnutzer umsetzen. [REQ.FAKAT.ConServices.30]
Bereitstellen der Zertifikate des SMGW	Das SMGW **MUSS** ▸FA.ReadCertificate für den Anschlussnutzer umsetzen. [REQ.FAKAT.ConServices.40]
Löschen von Session-Schlüsseln (Logout), so dass eine erneute Authentifizierung gegenüber dem SMGW erforderlich wird	Das SMGW **SOLL** ▸FA.DoLogout für den Anschlussnutzer umsetzen. (▸ICS.FAKAT.ConServices.10) [REQ.HAN.SicherungKommunikationConSrv.20] [5]
Ändern des Endkunden-Passworts	Das SMGW **SOLL** ▸FA.DoChangeUserPassword für den Anschlussnutzer bereitstellen. (▸ICS.FAKAT.ClsServices.10) [REQ.FAKAT.ConServices.50]
Bereitstellung einer Startseite für eine browserbasierten Navigation, Darstellung und Konfiguration für den Endkunden	Das SMGW **SOLL** ▸FA.ReadStartPage für den Anschlussnutzer bereitstellen. (▸ICS.FAKAT.ClsServices.10) [REQ.FAKAT.ConServices.60]
Systemzeit zur Synchronisation bereitstellen	Das SMGW **SOLL** ▸FA.NtpTimeService für den Anschlussnutzer umsetzen. (▸ICS.FAKAT.ConServices.10) [REQ.FAKAT.ConServices.90]
Gerätestatus bereitstellen (SMGW, Messeinrichtung)	Das SMGW **KANN** ▸FA.ReadDeviceStatus für den Anschlussnutzer umsetzen. (▸ICS.FAKAT.ConServices.10)([REQ.FAKAT.ConServices.100]

Tabelle 3.20 Übersicht der FA der Kategorie FAKAT.ConServices

ICS



ICS.FAKAT.ConServices.10

Der GWH **MUSS** im ICS deklarieren welche FAs das SMGW für die Rolle CON unterstützt.



ICS.HAN.SicherungKommunikationConSrv.10

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

3.6.3 Datenstrukturen

Die Datenstruktur des Anschlussnutzer-Logs ist in ▸Abschnitt 3.22.26 beschrieben.

[5] Ausloggen bezeichnet das Beenden einer Authentifizierung des Nutzers auf Anwendungs- oder Transportsicherungsebene, so dass die in der TLS-Verbindung vereinbarten, gemeinsame Sitzungsschlüssel auf Anwendungs- oder Transportsicherungsebene nicht mehr verwendet werden können.

Die Datenstruktur zur Bereitstellung des Zeitsynchronisations-Status ist in ▸Abschnitt 3.22.47 beschrieben.

Die Datenstrukturen zur Bereitstellung der abrechnungsrelevanten Auswertungsprofile und Regelwerkparameter sind in ▸Abschnitt 3.22.6 und in den TAF-spezifischen Abschnitten der FA zur Messwertverarbeitung beschrieben.

Die Datenstruktur zur Bereitstellung der registrierten Werte (RWL) ist in ▸Abschnitt 3.22.35 beschrieben.

Die Datenstruktur zur Bereitstellung der historischen Tageswerte (TWL) ist in ▸Abschnitt 3.22.43 beschrieben.

Die Datenstruktur zur Bereitstellung der aktuellen (vom Zähler empfangenen) Werte ist in ▸Abschnitt 3.22.5 beschrieben.

Die Datenstruktur zur Bereitstellung der abgeleiteten Werte (AWL) ist in ▸Abschnitt 3.22.4 beschrieben.

3.6.4 FA.ExportUserLog

3.6.4.1 Beschreibung

Dieser FA exportiert das Anschlussnutzer-Log des authentifizierten, berechtigten Nutzers. Dem über das Datenfeld "userId" im Auswertungsprofil und im HAN-Konfigurationsprofil identifizierten Nutzer ist ein Anschlussnutzer-Log mit der gleichen "userId" zugeordnet.

Sofern im Auswertungsprofil zusätzlich eine dem Anschlussnutzer bzw. Anlagenbetreiber zugeordnete "clsId" konfiguriert ist, werden die in das USER-Log (siehe Anhang) zu protokollierenden Ereignisse die das CLS betreffen über das Anschlussnutzer-Log exportiert.

Das SMGW protokolliert im Anschlussnutzer-Log Ereignisse gemäß ▸Anhang A:

- Änderungen an dem Anschlussnutzer zugeordneten Auswertungsprofilen und LMN-Kommunikationsprofilen
- Erfolgreicher Versand von dem Anschlussnutzer zugeordneten Messwerten an berechtigte externe Entitäten
- Den Anschlussnutzer betreffende administrative Handlungen (Anlegen, Ändern, Löschen, Auslesen von Konfigurationsprofilen)
- Für den Anschlussnutzer relevante Systeminformation und Fehler
- Die Kennung des Anschlussnutzers
- Die eindeutige Kennung der am SMGW angeschlossenen, dem Anschlussnutzer zugeordneten Messeinrichtungen und Zählpunktbezeichnungen/Messlokations-IDs
- Identifikation von aktiven und geänderten Auswertungs- und LMN-Kommunikationsprofilen, die dem Anschlussnutzer zugeordnet sind
- Identifikation der über dem Anschlussnutzer zugeordneten Auswertungsprofilen berechtigten Messwertempfängern
- Abrechnungsrelevante Status- und Fehlermeldungen des SMGW und der dem Anschlussnutzer zugeordneten Messeinrichtungen
- Historische Tarifstufenwechsel

Query-Parameter gemäß [DS] Kapitel "RESTful Webservices" Abschnitt "Query-Parameter" können die exportierte Datenmenge mindestens nach Zeitraum und Ereignistyp begrenzen.

Hinweis: Die versandten Messwerte und Tarifinformationen werden nicht über diesen FA bereitgestellt.

3.6.4.2 Auslöser



REQ.FA.ExportUserLog.120

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle CON.
- Empfang einer Anfrage über ▸HKS.WS2 in der Rolle CON.

3.6.4.3 Anforderungen

- Das SMGW **MUSS** das Anschlussnutzer-Log exportieren, das dem durch das HAN-Kommunikationsprofil identifizierten Anschlussnutzer ▸userId zugeordnet ist. [REQ.FA.ExportUserLog.10]
- Das SMGW **SOLL** über Abfrageparameter den Zeitraum (Von-Bis) der ausgelesenen Logeinträge eingrenzen können. [REQ.FA.ExportUserLog.20]
- Das SMGW **SOLL** über Abfrageparameter die Anzahl der ausgelesenen Logeinträge begrenzen können. [REQ.FA.ExportUserLog.30]
- Sofern kein Abfrageparameter die Anzahl der ausgelesenen Logeinträge begrenzt, **MUSS** das SMGW nicht mehr als 1000 Logeinträge exportieren. [REQ.FA.ExportUserLog.31]
- Das SMGW **SOLL** die exportierten Logeinträge über einen Abfrageparameter auf eine Ereignis-ID (Tupel Vendor.EventID.EventSubId) eingrenzen können. [REQ.FA.ExportUserLog.40]
- Das SMGW **MUSS** unbekannte Abfrageparameter ignorieren. [REQ.FA.ExportUserLog.50]
- Das SMGW **MUSS** die Informationen gemäß ▸Logbuch und Ereignisse bereitstellen. [REQ.FA.ExportUserLog.60]
- Das SMGW **SOLL** älteste Logeinträge zuerst übertragen, sofern ein Abfrageparameter nicht etwas anderes festlegt. [REQ.FA.ExportUserLog.70]
- Das SMGW **SOLL** die exportierten Logeinträge über einen Abfrageparameter auf einen "Level" (I, W, E, F) einschränken können. [REQ.FA.ExportUserLog.80]
- Das SMGW **MUSS** die ▸profileId des Logbuches in der Export-Struktur aus der ▸userId des authentifizierten Nutzers übernehmen. [REQ.FA.ExportUserLog.110]
- Sofern der Aufrufparameter "q.signed=CMS_ECDSA_SHA256_Detached" oder "q.signed" einen signierten Export des Logs anfordert, **MUSS** das SMGW die Export-Signatur ▸signature.sigValue über die kanonisierten Datenfelder der Export-Struktur mit dem Algorithmus CMS_ECDSA_SHA256_Detached und dem Signaturschlüssel des SMGW (GW_WAN_SIG_PRV) berechnen. Das Datenfeld ▸signature.sigValue selbst geht nicht in die Signaturberechnung ein. [REQ.FA.ExportUserLog.100]
- Das SMGW **MUSS** das UserLog gemäß ▸Tabelle 3.49 in der Export-Struktur ▸Exportstruktur an den Aufrufer übermitteln. [REQ.FA.ExportUserLog.90]

ICS



ICS.FA.ExportUserLog.10

Der GWH **MUSS** im ICS deklarieren, welche Filterparameter zur Begrenzung der exportieren Logeinträge ausgewertet werden.

3.6.5 FA.ReadInstantMtrReading

3.6.5.1 Beschreibung

Ein Aufrufparameter bestimmt die Zähler-ID, für den die aktuellen Eingangsmesswerte bereitgestellt werden sollen. Die Zähler-ID muss dem aufrufenden, authentifizierten Nutzer über mindestens ein Auswertungsprofil zugeordnet sein. Siehe dazu die Abbildung in ▸FAKAT.ValProcConfig.

Das SMGW stellt die letzten authentisch empfangenen Messwerte gemäß der Vereinigungsmenge der zu erfassenden OBIS-IDs (▸meterReadingInput) aller dem Nutzer zugeordneten Auswertungsprofile zu diesem Zähler bereit. Darüber hinaus wird die von der Messeinrichtung gemessene Momentanleistung (OBIS-Kennzahl 1-0:16.7.0) und der aktuelle Zählerstand (OBIS-Kennzahl 1-0:1.8.0 und 1-0:2.8.0) bereitgestellt, sofern die Messeinrichtung diese Werte liefert.

Die Aktualität der bereitgestellten Messwerte ist idealerweise kleiner als 1 % der Registrierperiode inklusive einer angenommenen Verzögerung von 2 Sekunden zwischen Messung und Empfangszeitstempel, höchstens aber die vom Hersteller im ICS angegebene Aktualität.

Das so über "userId" und "meterId" identifizierte Auswertungsprofil wird als Grundlage der folgenden Anforderungen referenziert.

Eine Liste von Query-Parametern (z.B. q.obis=1-0:1.8.0) kann die Bereitstellung der Eingangsmesswerte auf bestimmte OBIS-IDs einschränken.

3.6.5.2 Auslöser



REQ.FA.ReadInstantMtrReading.40

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle CON oder CLS.
- Empfang einer Anfrage über ▸HKS.WS2 in der Rolle CON.

3.6.5.3 Anforderungen

- Das SMGW **MUSS** den Aufruf ablehnen, wenn kein Auswertungsprofil für die ▸userId des aufrufenden, authentifizierten Nutzers konfiguriert ist oder keines ein LMN-Kommunikationsprofil referenziert, dessen ▸meterId mit dem Aufrufparameter übereinstimmt. [REQ.FA.ReadInstantMtrReading.10]
- Das SMGW **MUSS** alle per OBIS-ID identifizierten Messgrößen exportieren, die in ▸meterReadingInput der Auswertungsprofile des anfragenden Nutzers (▸userId) für die angefragte "meterId" festgelegt sind. Bei Mehrfachkonfiguration identischer OBIS-IDs wird die Messgröße nur einmal ausgegeben. [REQ.FA.ReadInstantMtrReading.15]
- Das SMGW **SOLL** für bidirektional kommunizierende Messeinrichtungen die aktuellen Messwerte für mindestens die OBIS-Kennzahlen nach ▸Tabelle 3.21 für die angefragte "meterId" bereitstellen, sofern die Messeinrichtung diese Messgrößen bereitstellt. (▸ICS.FA.ReadInstantMtrReading.20) [REQ.FA.ReadInstantMtrReading.50]
- Das SMGW **SOLL** für unidirektional kommunizierende Messeinrichtungen die aktuellen Messwerte für alle OBIS-Kennzahlen für die angefragte "meterId" bereitstellen, die von der Messeinrichtung geliefert werden. (▸ICS.FA.ReadInstantMtrReading.40) [REQ.FA.ReadInstantMtrReading.60]
- Sofern die angefragte "meterId" einen bidirektional kommunizierenden Zähler (LKS1) identifiziert und der Empfangszeitpunkt der zuletzt empfangenen Messwerte länger als die Dauer gemäß ▸ICS.FA.ReadInstantMtrReading.10 zurückliegt, **MUSS** das SMGW aktuelle Messwerte für die zu berücksichtigenden Messgrößen abfragen (Siehe ▸FA.CaptureRequestedMtrData). [REQ.FA.ReadInstantMtrReading.20]
- Das SMGW **SOLL** eine Aktualität der über diesen FA bereitgestellten Messwerte von 7 Sekunden oder kürzer nach Empfangszeitstempel gewährleisten. [REQ.FA.ReadInstantMtrReading.25]
- Das SMGW **MUSS** für alle zu berücksichtigenden Messgrößen die zuletzt empfangenen Messwerte gemäß ▸Eingangsmesswerte unter Berücksichtigung der Einschränkung durch Query-Parameter an den Aufrufer exportieren. [REQ.FA.ReadInstantMtrReading.30]

OBIS-Kennzahl	Beschreibung
Elektrische Energie	
1-0:1.8.0	Verbrauchszählerstand
1-0:2.8.0	Einspeisezählerstand
1-0:16.7.0	Wirkleistung gesamt
1-0:36.7.0	Wirkleistung L1
1-0:56.7.0	Wirkleistung L2
1-0:76.7.0	Wirkleistung L3

Tabelle 3.21 Für LKS1 Messeinrichtungen zusätzlich bereitzustellende Messgrößen

ICS



ICS.FA.ReadInstantMtrReading.10

Der GWH **MUSS** im ICS beschreiben, welche Aktualität (in Sekunden) für über diesen FA bereitgestellte Messwerte bei bidirektional angebundenen Messeinrichtungen gewährleistet wird. Die Ak-

tualität wird ausgehend vom Empfangszeitstempel im SMGW bestimmt. Der Wert muss zwischen 1 und 60 Sekunden liegen.



ICS.FA.ReadInstantMtrReading.20

Der GWH **MUSS** im ICS beschreiben, ob das SMGW für bidirektional kommunizierende Messeinrichtungen die Messgrößen nach ▸Tabelle 3.21 bereitstellen kann.



ICS.FA.ReadInstantMtrReading.40

Der GWH **MUSS** im ICS beschreiben, ob das SMGW alle von unidirektional kommunizierenden Messeinrichtungen gelieferten Messgrößen bereitstellen kann.

3.6.5.4 Implementierungshinweis

Der Hersteller sorgt durch Verzögern der Antwort bis höchstens zur Schwelle der garantierten Aktualität ▸ICS.FA.ReadInstantMtrReading.10 dafür, dass keine Überlastung des SMGWs durch zu häufige Abfragen (Polling) stattfinden kann (z.B. durch Verzögerung der Antwort). Insbesondere muss die Einhaltung der Sollregistrierzeitpunkte (Siehe ▸Abschnitt 3.2.4) gewährleistet bleiben.

3.6.6 FA.ExportRegMtrReading

3.6.6.1 Beschreibung

Das SMGW exportiert die registrierten Werte gemäß ▸RWL.

Ein Aufrufparameter ("meterId") identifiziert die Messeinrichtung, deren registrierte Messwerte bereitgestellt werden sollen.

Das SMGW stellt die registrierten und im SMGW gespeicherten Messwerte dem Nutzer für den Zeitraum bereit, in dem dieser Nutzer gemäß (gültigem oder archiviertem) Auswertungsprofil berechtigt ist die Messwerte eines Zählers zu erhalten.

Die Messwerte werden mit Zähler-Identifikation, Zeitstempel, OBIS-Kennzahl und verkehrsgebräuchlicher Einheit (kWh, kvarh, m^3) exportiert.

Ein Aufrufparameter bestimmt die Zähler-ID.

Query-Parameter gemäß [DS] Kapitel "RESTful Webservices" Abschnitt "Query-Parameter" können die exportierte Datenmenge mindestens nach Zeitraum begrenzen.

Über einen Aufrufparameter kann bestimmt werden, ob über die exportierten Messwerte eine Signatur mit dem GW_WAN_SIG_CRT gebildet wird.

Die Aufbewahrungsfristen für registrierte Werte werden in ▸Abschnitt 5.5 beschrieben.

3.6.6.2 Auslöser



REQ.FA.ExportRegMtrReading.100

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle CON.
- Empfang einer Anfrage über ▸HKS.WS2 in der Rolle CON.

3.6.6.3 Anforderungen

- Das SMGW **MUSS** die exportierten Messwerte auf den Zeitraum begrenzen, der dem Gültigkeitszeitraum ▸validityPeriod des gültigen oder archivierten Auswertungsprofils des authentifizierten Nutzers (▸userId) entspricht. [REQ.FA.ExportRegMtrReading.60]
- Das SMGW **MUSS** den Export ablehnen, wenn der Aufrufparameter keine Messeinrichtung identifiziert, die in einem Auswertungsprofil des identifizierten Nutzers (▸userId) referenziert wird. [REQ.FA.ExportRegMtrReading.20]

- Das SMGW **MUSS** die Zählerstände der RWL gemäß ▸Exportstruktur für die Datenstruktur ▸Registrierter Wert und registrierte Wertliste (RWL) mit den OBIS-IDs (▸Identifikation der vom SMGW bereitgestellten Messgrößen), Einheiten und das kombinierte Statuswort (Siehe ▸Kombiniertes Statuswort) an den Aufrufer exportieren. [REQ.FA.ExportRegMtrReading.30]
- Sofern Aufrufparameter zur Begrenzung der exportierten Datenmenge vorhanden sind, **SOLL** das SMGW den Export der registrierten Werte entsprechend der Aufrufparameter gemäß [DS] Kapitel "RESTful Webservice" Abschnitt "Query Parameter" begrenzen. (▸ICS.FA.ExportRegMtrReading.10). [REQ.FA.ExportRegMtrReading.40]
- Das SMGW **MUSS** die exportierten Messwertsätze gemäß ▸Tabelle 3.22 in der Export-Struktur ▸Abschnitt 3.22.17 an den Aufrufer übermitteln. [REQ.FA.ExportRegMtrReading.80]
- Sofern der Aufrufparameter "q.signed=CMS_ECDSA_SHA256_Detached" oder "q.signed" einen signierten Export der Messwerte anfordert, **MUSS** das SMGW die Export-Signatur ▸signature.sigValue über die kanonisierten Datenfelder der Export-Struktur mit dem Algorithmus CMS_ECDSA_SHA256_Detached, dem Signaturschlüssel des SMGW (GW_WAN_SIG_PRV) berechnen. Das Datenfeld ▸signature.sigValue selbst geht nicht in die Signaturberechnung ein. [REQ.FA.ExportRegMtrReading.50]
- Das SMGW **MUSS** registrierte Werte über einen Zeitraum gemäß den Vorhaltefristen in ▸Abschnitt 5.5 bereitstellen können. [REQ.FA.ExportRegMtrReading.70]

Export Datenfeld	Ursprung
▸exportedData	Siehe ▸Tabelle 3.100
▸tafId	Anwendungsreferenz aus dem gleichnamigen Datenfeld des mit dem Aufrufparameter "meterId" verknüpften Auswertungsprofiles ▸meterReadingInput.meterId).
▸gatewayId	Der SubjectCN des GW_WAN_TLS_CRT (entspricht dem SubjectCN des GW_WAN_SIG_CRT)
▸signature	Entfällt, sofern gemäß ▸REQ.FA.ExportRegMtrReading.50 keine Signatur erstellt wird.
▸signature.ts	Systemzeit des SMGW beim Aufruf (Signaturerstellungszeitpunkt)
▸signature.algo	Gemäß in ▸REQ.FA.ExportRegMtrReading.50 verwendetem Algorithmus
▸signature.originator	Die HÜID des SubjectCN des GW_WAN_SIG_CRT
▸signature.sigValue	Codierung und Wert gemäß in ▸REQ.FA.ExportRegMtrReading.50 verwendetem Verfahren

Tabelle 3.22 Übernahme von Datenfeldern in die exportierte Registrierte Werteliste

ICS



ICS.FA.ExportRegMtrReading.10

Der Hersteller **MUSS** im ICS beschreiben, über welche Query-Parameter der Export von registrierte Werte begrenzt werden kann.



ICS.FA.ExportRegMtrReading.20

Der Hersteller **MUSS** im ICS beschreiben, ob ein signierter Export von registrierten Werten unterstützt wird.

3.6.7 FA.ExportDailyMtrReading

3.6.7.1 Beschreibung

Das SMGW exportiert die zum Tageswechsel gespeicherten Messwerte (auch als "Tageswertliste" bezeichnet, siehe auch ▸Abschnitt 3.2.5) gemäß ▸TWL.

Ein Aufrufparameter identifiziert den Zähler und optional den Zeitraum, dessen Tageswerte bereitgestellt werden sollen.

Das SMGW stellt die Messwerte dem identifizierten und authentifizierten Nutzer für den Zeitraum bereit, in dem dieser Nutzer gemäß (gültigem oder archiviertem) Auswertungsprofil berechtigt ist die Messwerte eines Zählers zu erhalten.

Die Messwerte werden mit Zähler-Identifikation, Zeitstempel, OBIS-Kennzahl und verkehrsgebräuchlicher Einheit (kWh, kvarh, m^3) exportiert.

Query-Parameter gemäß [DS] Kapitel "RESTful Webservices" Abschnitt "Query-Parameter" können die exportierte Datenmenge begrenzen.

Das SMGW speichert historische Werte, indem täglich (zum Tagesende gemäß Auswertungsprofil) der letzte von der Messeinrichtung empfangenen Zählerstand gespeichert wird.

Das SMGW stellt dem authentifizierten Anschlussnutzer die historischen Zählerstände lokal bereit. Aus zwei Zählerständen kann der Anschlussnutzer durch Differenzbildung die tages-, wochen-, monats- und jahresbezogenen Energieverbrauchs- oder Einspeisemengen bestimmen.

Dabei können über Aufrufparameter (Query-Parameter) die zu exportierenden Zählerstände mindestens nach Zeitraum, Zähler-ID und OBIS-ID begrenzt werden. "q.latest" liefert den letzten Tageszählerstand.

Die Vorhaltefristen für Tageswerte sind in ▸Abschnitt 5.5 beschrieben.

3.6.7.2 Auslöser



REQ.FA.ExportDailyMtrReading.90

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle CON.
- Empfang einer Anfrage über ▸HKS.WS2 in der Rolle CON.

3.6.7.3 Anforderungen

- Das SMGW **MUSS** den Export ablehnen, wenn der Aufrufparameter keine Messeinrichtung identifiziert, die in einem (gültigen oder archivierten) Auswertungsprofil des identifizierten Nutzers (▸userId) referenziert wird. [REQ.FA.ExportDailyMtrReading.60]
- Das SMGW **MUSS** die exportierten Messwerte auf den Zeitraum begrenzen, der dem Gültigkeitszeitraum ▸validityPeriod des gültigen oder archivierten Auswertungsprofils des authentifizierten Nutzers (▸userId) entspricht. [REQ.FA.ExportDailyMtrReading.50]
- Das SMGW **SOLL** über Aufrufparameter (Queryparameter) die exportieren Datensätze begrenzen können. [REQ.FA.ExportDailyMtrReading.20]
- Sofern der Aufrufparameter "q.signed=CMS_ECDSA_SHA256_Detached" oder "q.signed" einen signierten Export anfordert, **MUSS** das SMGW die Export-Signatur ▸signature.sigValue über die kanonisierten Datenfelder der Export-Struktur mit dem Algorithmus CMS_ECDSA_SHA256_Detached, dem Signaturschlüssel des SMGW (GW_WAN_SIG_PRV) berechnen. Das Datenfeld ▸signature.sigValue selbst geht nicht in die Signaturberechnung ein. [REQ.FA.ExportDailyMtrReading.80]
- Das SMGW **MUSS** Tageswerte über einen Zeitraum gemäß den Vorhaltefristen in ▸Abschnitt 5.5 bereitstellen können, so dass der Anschlussnutzer daraus historische tages-, wochen-, monats- und jahresbezogene Energieverbrauchs- oder Einspeisewerte bestimmen kann. [REQ.HAN.AnschlussnutzerDatenbereitstellung.71]
- Das SMGW **MUSS** die Datenfelder der Export-Datenstruktur und der exportierten TWL gemäß ▸Tabelle 3.23 setzen. [REQ.FA.ExportDailyMtrReading.70]
- Das SMGW **MUSS** die, vom im Aufrufparameter referenzierten Zähler erfassten Tageswerte gemäß ▸Abschnitt 3.22.43 in der Export-Struktur ▸Abschnitt 3.22.17 als DailyMeterReadingList an den Aufrufer exportieren. [REQ.FA.ExportDailyMtrReading.30]

Export Datenfeld	Ursprung
▸exportedData	Siehe ▸Tabelle 3.108

Export Datenfeld	Ursprung
▸tafId	Anwendungsreferenz aus dem gleichnamigen Datenfeld des mit dem Aufrufparameter "meterId" verknüpften Auswertungsprofiles ▸meterReadingInput.meterId.
▸gatewayId	Der SubjectCN des GW_WAN_TLS_CRT (entspricht dem SubjectCN des GW_WAN_SIG_CRT)
▸signature	Entfällt, sofern gemäß ▸REQ.FA.ExportDailyMtrReading.80 keine Signatur erstellt wird.
▸signature.ts	Systemzeit des SMGW beim Aufruf (Signaturerstellungszeitpunkt)
▸signature.algo	Gemäß in ▸REQ.FA.ExportDailyMtrReading.80 verwendetem Algorithmus
▸signature.originator	Die HÜID des SubjectCN des GW_WAN_SIG_CRT
▸signature.sigValue	Codierung und Wert gemäß in ▸REQ.FA.ExportDailyMtrReading.80 verwendetem Verfahren

Tabelle 3.23 Übernahme von Datenfeldern in die exportierte Tageswertliste

ICS

ICS.FA.ExportDailyMtrReading.10

Der Hersteller **MUSS** im ICS beschreiben, über welche Query-Parameter der Export von Tageswerten begrenzt werden kann.

3.6.8 FA.DoChangeUserPassword

3.6.8.1 Beschreibung

Dieser FA ermöglicht dem lokalen, über Benutzername und Passwort authentifizierten Endkunden, sein Authentifizierungspasswort zur Anmeldung an der HAN-Schnittstelle des SMGW zu ändern. Der Aufrufparameter enthält das neue Passwort und eine Passwort-Wiederholung, um Tippfehler zu erkennen.

3.6.8.2 Auslöser

REQ.FA.DoChangeUserPassword.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸HKS.WS2 in der Rolle CON.

3.6.8.3 Anforderungen

- Das SMGW **MUSS** den Aufruf ablehnen, wenn die Inhalte der Datenfelder ▸password und ▸passwordRepeat nicht übereinstimmen. [REQ.FA.DoChangeUserPassword.20]
- Das SMGW **MUSS** den Aufruf ablehnen, wenn das Passwort ▸password nicht die Mindestlänge hat. (▸ICS.FA.DoChangeUserPassword.10) [REQ.FA.DoChangeUserPassword.50]
- Das SMGW **MUSS** den Hash H(A1) über (Realm (kanonisierte SMGW-ID gemäß ▸Abschnitt 5.3 entsprechend dem SubjectCN des GW_WAN_TLS_CRT, lowercase), ▸userCredentials.username und ▸password) gemäß [DS] Kapitel "HTTP-Authentifizierungs-Protokoll" für alle ▸userCredentials.authScheme des der auslösenden Verbindung zugeordneten HAN-Kommunikationsprofiles berechnen. [REQ.FA.DoChangeUserPassword.40]
- Das SMGW **MUSS** den oder die berechneten Hashes H(A1) in ▸userCredentials.hash des zur Authentifizierung verwendeten HAN-Kommunikationsprofil persistieren und künftig für die Authentifizierung mit dem HAN-Kommunikationsprofil verwenden. ▸ [BSI.20033.0] [REQ.FA.DoChangeUserPassword.30]

ICS

ICS.FA.DoChangeUserPassword.10

Der GWH **MUSS** im ICS deklarieren, unterhalb welcher Mindestlänge das SMGW die Passwörter ablehnt. Ein Wert kleiner 4 ist nicht zulässig.

3.6.8.4 Implementierungshinweise

Der Aufrufparameter wird mit dem Content-Type "application/x-www-form-urlencoded" an das SMGW übermittelt, um eine Eingabe der Datenfelder im Browser zu ermöglichen.

Das übermittelte Passwort wird nach der Berechnung des Hashes gelöscht.

Passwörter oder PINs sollten gemäß Stand der Technik eine ausreichende Stärke für die Einsatzumgebung der HAN-Schnittstelle besitzen.

3.6.9 FA.DoLogout

3.6.9.1 Beschreibung

Dieser FA ermöglicht es, die (TLS-)Session der Verbindung, über die der Nutzer authentifiziert ist, vorzeitig zu beenden, so dass eine erneute Authentifizierung erforderlich ist.

3.6.9.2 Auslöser



REQ.FA.DoLogout.30

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle CON.
- Empfang einer Anfrage über ▸HKS.WS2 in der Rolle CON, CLS, SRV.
- Unmittelbar nach Ablauf von 10 Minuten ohne TLS-Applikationsdatentransfer für die Rolle CON und SRV.

3.6.9.3 Anforderungen

Das SMGW **MUSS** die, der auslösenden TLS-Verbindung zugeordneten, gemeinsamen Sitzungsschlüssel löschen und die Verbindung beenden. [REQ.FA.DoLogout.10]

Sofern der FA über HKS.WS2 ausgelöst wurde, **MUSS** das SMGW den Kommunikationspartner beim nächsten FA-Aufruf über eine erneute (Challenge/Response)-HTTP-Authentifizierung authentifizieren. [REQ.FA.DoLogout.20]

3.6.10 FA.ReadStartPage

3.6.10.1 Beschreibung

Dieser FA ermöglicht es dem Anschlussnutzer, über seinen Browser eine vom SMGW erzeugte Startseite abzurufen, die ihm das einfache Ändern seines Passwortes erlaubt und ohne spezielle Anwendungssoftware seine Daten im Browser darstellt.

Nr.	Information
1	Software-Identifikation des SMGW, inklusive der metrologischen Softwareteile,
2	aktueller Zählerstand der dem authentifizierten Nutzer zugeordneten Messeinrichtungen,
3	aktueller Energiemengenregister der dem authentifizierten Nutzer zugeordneten Messeinrichtungen,
4	aktuelle Tarifstufe der dem authentifizierten Nutzer zugeordneten Auswertungsprofile mit Tarifstufen,
5	aktuelle Systemzeit des SMGW mit lokaler Zeitzone,
6	historische Verbrauchswerte der dem authentifizierten Nutzer zugeordneten Messeinrichtungen,
7	aktuelles und ggf. vorheriges SMGW-Signaturzertifikat (GW_WAN_SIG_CRT) zur Validierung exportierter Daten,
8	eine Formularseite zur Änderung des Passwortes des authentifizierten Nutzers,
9	die aktuellsten Einträge des UserLogs,
10	eine Möglichkeit zum Ausloggen, so dass eine erneute HTTP-Digest-Authentifizierung angefordert wird.

Tabelle 3.24 Bereitgestellte Informationen

3.6.10.2 Auslöser

REQ.FA.ReadStartPage.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle CON.
- Empfang einer Anfrage über ▸HKS.WS2.

3.6.10.3 Anforderungen

- Das SMGW **MUSS** als Antwort auf die HTTP-Anfrage "GET /" ein nach aktuellem Standard syntaktisch korrektes HTML-Dokument bereitstellen. [REQ.FA.ReadStartPage.20]
- Das SMGW **MUSS** eine Formularseite zur Eingabe des zu ändernden Passworts (mit Passwortwiederholung) anzeigen (Zwei Eingabefelder mit jeweils mind. 40 Zeichen) (siehe ▸FA.DoChangeUserPassword). [REQ.FA.ReadStartPage.30]
- Das SMGW **MUSS** für das GW_HAN_SIG_CRT und GW_HAN_SIG_CRT_PREV jeweils einen Download-Link bereitstellen (siehe ▸FA.ReadCertificate). [REQ.FA.ReadStartPage.40]
- Das SMGW **MUSS** einen Link für den signierten Export von Teilen des Anschlussnutzer-Logs bereitstellen (siehe ▸FA.ExportUserLog). [REQ.FA.ReadStartPage.50]
- Das SMGW **MUSS** einen Link für den signierten Export von Registrierten Messwertlisten bereitstellen (siehe ▸FA.ExportRegMtrReading). [REQ.FA.ReadStartPage.60]
- Das SMGW **MUSS** einen Link für den signierten Export von Abgeleiteten Messwertlisten bereitstellen (siehe ▸FA.ExportDerivedMtrReading). [REQ.FA.ReadStartPage.70]
- Das SMGW **MUSS** einen Link für den Export von Tageswertlisten bereitstellen (siehe ▸FA.ExportDailyMtrReading). [REQ.FA.ReadStartPage.80]

3.6.10.4 Implementierungshinweise

Der aktuelle Stand der HTML-Spezifikation ist bei der W3C abrufbar. Empfohlen wird HTML5.

Um eine ergonomische Darstellung zu erhalten, sollten die Informationen strukturiert und mit CSS mit lesbarem Schriftstil, Schriftgröße und kontrastreicher Farbe angezeigt werden.

Empfohlen wird eine Beschreibung mindestens in deutscher und englischer Sprache.

Zur strukturierten und lesbaren Darstellung sollte die Navigation thematische Unterseiten verwenden.

Bei der Auswahl der ausgelieferten Webseiten-Elemente sollte die Unterstützung durch die aktiv weiterentwickelten HTML-Renderer der verbreiteten Betriebssysteme berücksichtigt werden.

3.6.11 FA.ExportDerivedMtrReading

3.6.11.1 Beschreibung

Das SMGW stellt dem identifizierten und authentifizierten Anschlussnutzer den Inhalt der einem Auswertungsprofil zugeordneten abgeleiteten Werteliste (AWL) für den Zeitraum bereit, in dem dieser Anschlussnutzer gemäß (gültigem oder archiviertem) Auswertungsprofil berechtigt ist, diese abgeleiteten Messwerte zu erhalten. Der Aufrufer kann den Export auf einen Zeitraum begrenzen. Die AWL enthält die abgeleiteten Werte der vorangegangenen Abrechnungsperioden und den aktuellen Registerstand der aktuellen Abrechnungsperiode.

Ein Aufrufparameter bestimmt das Auswertungsprofil.

Query-Parameter gemäß [DS] Kapitel "RESTful Webservices" Abschnitt "Query-Parameter" können die exportierte Datenmenge begrenzen.

Der Aufrufparameter "q.latest" liefert den aktuellen Stand der Zählregister.

Die Vorhaltefristen abgeleiteter Wertelisten und der Auswertungsprofile sind in ▸Abschnitt 5.5 beschrieben.

3.6.11.2 Auslöser



REQ.FA.ExportDerivedMtrReading.90

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle CON.
- Empfang einer Anfrage über ▸HKS.WS2 in der Rolle CON.

3.6.11.3 Anforderungen

- Sofern der Aufrufparameter ein Auswertungsprofil identifiziert, **MUSS** das SMGW die Export-Anfrage ablehnen, wenn das über Aufrufparameter identifizierte Auswertungsprofil nicht für den authentifizierten Anschlussnutzer (▸userId) gültig oder archiviert vorliegt. [REQ.FA.ExportDerivedMtrReading.10]
- Das SMGW **MUSS** die exportierten Messwerte auf den Zeitraum begrenzen, der dem Gültigkeitszeitraum ▸validityPeriod des gültigen oder archivierten Auswertungsprofils des authentifizierten Nutzers (▸userId) entspricht. [REQ.FA.ExportDerivedMtrReading.30]
- Das SMGW **MUSS** die Zählerstände der AWL gemäß ▸Exportstruktur für die Datenstruktur ▸Abgeleiteter Wert und Liste abgeleiteter Werte (AWL) mit den OBIS-IDs (▸Identifikation der vom SMGW bereitgestellten Messgrößen), Einheiten und das kombinierte Statuswort (Siehe ▸Kombiniertes Statuswort) an den Aufrufer exportieren. [REQ.FA.ExportDerivedMtrReading.40]
- Sofern Aufrufparameter zur Begrenzung der exportierten Datenmenge vorhanden sind, **SOLL** das SMGW den Export der abgeleiteten Werte entsprechend der Aufrufparameter gemäß [DS] Kapitel "RESTful Webservice" Abschnitt "Query Parameter" begrenzen. (▸ICS.FA.ExportDerivedMtrReading.10). [REQ.FA.ExportDerivedMtrReading.50]
- Das SMGW **MUSS** die Datenfelder der Export-Datenstruktur und der exportierten AWL gemäß ▸Tabelle 3.25 setzen. [REQ.FA.ExportDerivedMtrReading.60]
- Sofern ein Aufrufparameter zum signierten Export der abgeleiteten Messwerte vorhanden ist ("q.signed"), **SOLL** das SMGW die Abgeleitete Messwertliste mit dem privaten Schlüssel GW_WAN_SIG_PRV und dem Signatur-Verfahren gemäß [TR-03109-3] signieren und in der ▸Abschnitt 3.22.17 exportieren. (▸ICS.FA.ExportDerivedMtrReading.20) [REQ.FA.ExportDerivedMtrReading.70]
- Das SMGW **MUSS** abgeleitete Werte über einen Zeitraum gemäß den Vorhaltefristen in ▸Vorhaltefristen bereitstellen können. [REQ.FA.ExportDerivedMtrReading.80]

Export Datenfeld	Ursprung
▸tafId	Anwendungsreferenz aus dem gleichnamigen Datenfeld des mit der meterId verknüpften Auswertungsprofiles.
▸gatewayId	Der SubjectCN des GW_WAN_TLS_CRT (entspricht dem SubjectCN des GW_WAN_SIG_CRT)
▸signature	Entfällt, sofern gemäß ▸REQ.FA.ExportDerivedMtrReading.70 keine Signatur erstellt wird.
▸signature.ts	Systemzeit des SMGW beim Aufruf (Signaturerstellungszeitpunkt)
▸signature.algo	Gemäß in ▸REQ.FA.ExportDerivedMtrReading.70 verwendetem Algorithmus
▸signature.originator	Die HÜID des SubjectCN des GW_WAN_SIG_CRT
▸signature.sigValue	Codierung und Wert gemäß in ▸REQ.FA.ExportDerivedMtrReading.70 verwendetem Verfahren

Tabelle 3.25 Übernahme von Datenfeldern in die exportierte Abgeleitete Werteliste

ICS



ICS.FA.ExportDerivedMtrReading.10

Der Hersteller **MUSS** im ICS beschreiben, über welche Query-Parameter der Export von abgeleiteten Werte begrenzt werden kann.



ICS.FA.ExportDerivedMtrReading.20

Der Hersteller **MUSS** im ICS beschreiben, ob ein signierter Export von abgeleiteten Werten unterstützt wird.

3.6.12 FA.ReadTariffState

3.6.12.1 Beschreibung

Das SMGW stellt dem authentifizierten Nutzer für den laufenden Abrechnungsturnus bzw. die laufende Abrechnungsperiode die aktuellen Tarif-Informationen bereit. Die bereitgestellten Informationen bestimmen sich aus dem TAF:

- ▸TAF2: Aktuelle (Lokal-)Zeit, Inhalt aller Tarifstufenregister vom Beginn der Abrechnungsturnus bis zum letzten Sollregistrierzeitpunkt. Die aktuelle Zählzeitdefinition (gültig von-bis, Register, Beginn und Dauer/Ende der Abrechnungsperiode, Preisbestandteile).
- ▸TAF8: Aktuelle (Lokal-)Zeit, Ende des aktuellen Abrechnungsturnus, mittlere Leistung in der aktuellen Registrierperiode, maximale Leistung im aktuellen Abrechnungsturnus.

Dieser FA stellt die aktuellen Tarifstufen-Informationen bereit. Zurückliegende Tarifstufenwechsel werden in das UserLog protokolliert. Künftige Tarifstufenwechsel des ▸TAF2 können der Zählzeitdefinition des Auswertungsprofiles entnommen werden.

Aktuelle Tarifstufeninformationen können beispielsweise zur automatisierten Optimierung des Energieverbrauchs verwendet werden.

Ein Aufrufparameter identifiziert das Auswertungsprofil zu dem die aktuellen Tarifinformationen bereitgestellt werden.

3.6.12.2 Auslöser



REQ.FA.ReadTariffState.50

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle CON oder CLS.
- Empfang einer Anfrage über ▸HKS.WS2 in der Rolle CON.

3.6.12.3 Anforderungen

Das SMGW **MUSS** den Export ablehnen, wenn dem authentifizierten Aufrufer mit ▸userId kein ▸Auswertungsprofil vom Typ "▸TAF2" oder "▸TAF8" zugeordnet ist. [REQ.FA.ReadTariffState.10]



REQ.FA.ReadTariffState.30

(▸TAF2) Das SMGW **MUSS** dem authentifizierten Nutzer folgende zum Auslesezeitpunkt aktuelle Informationen übermitteln:

- Aktuelle Systemzeit zum Zeitpunkt der Erstellung der Datenstruktur (UTC mit lokalem Zeitoffset).
- Die Registerinhalte (Energiemengen) aller dem Auswertungsprofil zugeordneten Tarifstufenregister
- Der nächste Aktualisierungszeitpunkt (Ende des Abrechnungsturnus) gemäß Auswertungsprofil
- Die OBIS-ID des gemäß Zählzeitdefinition im Auswertungsprofil aktiven Tarifregisters
- Die Preisbestandteile der Tarifstufe, sofern diese im Auswertungsprofil konfiguriert sind
- Das kombinierte Statuswort (Siehe ▸Abschnitt 3.22.13) aus SMGW-Status und Status der dem Auswertungsprofil zugeordneten Messeinrichtung (Siehe ▸Abschnitt 3.22.28).

REQ.FA.ReadTariffState.40

(▸TAF8) Das SMGW **MUSS+** dem authentifizierten Nutzer folgende zum Auslesezeitpunkt aktuelle Informationen gemäß ▸Abschnitt 3.22.44 übermitteln:

- Aktuelle Systemzeit zum Zeitpunkt der Erstellung der Datenstruktur (UTC mit lokalem Zeitoffset).
- Den Registerinhalt (Mittlere Leistung) der in der letzten Registrierperiode bestimmten mittleren Leistung
- Den Registerinhalt (Maximale Leistung) der maximalen Leistung im Abrechnungsturnus
- Den Registerinhalt (Mittlere Leistung) der laufenden Registrierperiode
- Der nächste Aktualisierungszeitpunkt (Ende des aktuellen Abrechnungsturnus) gemäß Auswertungsprofil
- Den Beginn und das Ende des Abrechnungsturnus gemäß Auswertungsprofil
- Das kombinierte Statuswort (Siehe ▸Abschnitt 3.22.13) und den Status der dem Auswertungsprofil zugeordneten Messeinrichtung (Siehe ▸Abschnitt 3.22.28).

3.7 CLS-Dienste und Proxy-Funktionen (FAKAT.ClsServices)

3.7.1 Übersicht

Diese Anwendungsfallkategorie beschreibt die Dienste des SMGW für CLS. Dazu gehören die Anwendungsfälle zur Kommunikation eines CLS mit einem über den GWA autorisierten EMT im WAN und Dienste zur Zeitbereitstellung und CLS-Zertifikatserzeugung durch das SMGW.

Die notwendige Konfiguration zur Verwendung der Dienste durch ein CLS ist zweigeteilt. Die Proxy-Funktionalität zur Nutzung des Kommunikationskanals zu einem EMT wird über ein ▸Proxy-Kommunikationsprofil konfiguriert (siehe ▸FAKAT.ProxyConfig). Der Zugriff auf für CLS angebotene Dienste des SMGW wird über ein ▸HAN-Kommunikationsprofil mit ▸role "CLS" konfiguriert (siehe ▸FAKAT.HanUserConfig). Liegt eine der beiden Konfigurationen im SMGW nicht vor, kann das CLS die betroffene Funktionalität des SMGW nicht nutzen. Die zur Authentifizierung genutzten Informationen können für das CLS im ▸Proxy-Kommunikationsprofil und im ▸HAN-Kommunikationsprofil identisch sein.

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

▸Abbildung 3.13 zeigt die Funktion des Proxys zwischen CLS und EMT im WAN.

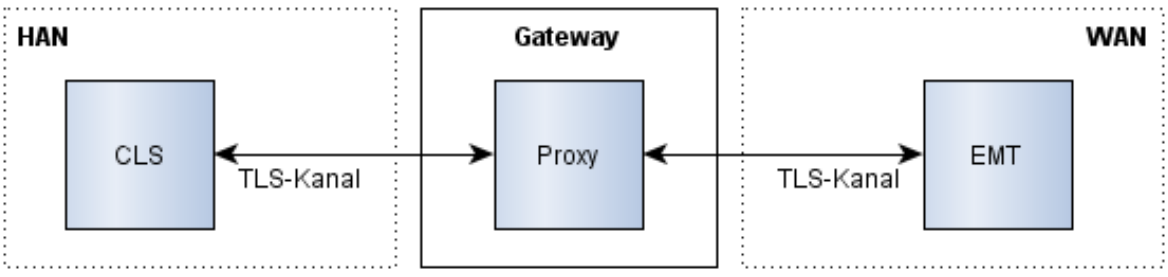


Abbildung 3.13. Proxy-Funktion zwischen CLS und EMT

3.7.2 Übersicht der FA

Aufgabe	Umsetzung
Aufbau eines transparenten Kommunikationskanals zwischen CLS und EMT, initiiert durch das CLS (bisher HKS3)	Das SMGW **MUSS** ▸FA.RequestProxyChByCls umsetzen. [REQ.HAN.HKS3.70]

Aufgabe	Umsetzung
Aufbau eines transparenten Kommunikationskanals zwischen CLS und EMT, initiiert durch den GWA (bisher HKS4)	Das SMGW **MUSS** ▸FA.DoRequestProxyCh für den GWA umsetzen. [REQ.WAN.Management.100]
Beendigung eines transparenten Kommunikationskanals zwischen CLS und EMT durch den GWA	Das SMGW **MUSS** ▸FA.DoCloseProxyCh für den GWA umsetzen. [REQ.WAN.Management.110]
Zeitgesteuerter Aufbau eines transparenten Kommunikationskanals zwischen CLS und EMT durch Konfigurationsbedingung im SMGW (bisher HKS5)	Das SMGW **MUSS** ▸FA.DoRequestProxyCh umsetzen. [REQ.HAN.HKS5.60]
Systemzeit zur Synchronisation bereitstellen	Das SMGW **MUSS** ▸FA.NtpTimeService für CLS umsetzen. [REQ.FAKAT.ClsServices.80]
Auslesen des dem CLS zugeordneten Zustandes des Proxy-Kommunikationskanals	Das SMGW **SOLL** ▸FA.ReadProxyChStatus für das CLS umsetzen. (▸ICS.FAKAT.ClsServices.10) [REQ.FAKAT.ClsServices.10]
Erzeugen eines Schlüsselpaares und Zertifikates für CLS	Das SMGW **MUSS** ▸FA.DoCreateKeyPairAndClsCert für das CLS umsetzen. [REQ.FAKAT.ClsServices.30]
Bereitstellung der letzten empfangenen Messwerte der dem CLS via "clsId" im Auswertungsprofil zugeordneten Zähler	Das SMGW **MUSS** ▸FA.ReadInstantMtrReading für das CLS umsetzen. [REQ.FAKAT.ClsServices.50]
Bereitstellung der dem CLS via "clsId" zugeordneten Auswertungsprofile und ihrer Tarif-Regelwerkparameter	Das SMGW **SOLL** ▸FA.ReadProcessingProfile (siehe ▸FAKAT.ValProcConfig) für das CLS umsetzen. (▸ICS.FAKAT.ClsServices.10) [REQ.FAKAT.ClsServices.60]
Bereitstellung der historischen registrierten Messwerte (RWL) der dem CLS via "clsId" zugeordneten Auswertungsprofile	Das SMGW **SOLL** ▸FA.ExportRegMtrReading für ein CLS umsetzen. (▸ICS.FAKAT.ClsServices.10) [REQ.FAKAT.ClsServices.120]
Bereitstellung der historischen Tageszählerständen (TWL) der dem CLS via "clsId" zugeordneten Auswertungsprofile	Das SMGW **SOLL** ▸FA.ExportDailyMtrReading für ein CLS umsetzen. (▸ICS.FAKAT.ClsServices.10) [REQ.FAKAT.ClsServices.130]
Bereitstellung der abgeleiteten Werte (AWL) der dem CLS via "clsId" zugeordneten Auswertungsprofile	Das SMGW **SOLL** ▸FA.ExportDerivedMtrReading für ein CLS umsetzen. (▸ICS.FAKAT.ClsServices.10) [REQ.FAKAT.ClsServices.140]
Bereitstellen der Zertifikate des SMGW	Das SMGW **MUSS** ▸FA.ReadCertificate für das CLS umsetzen. [REQ.FAKAT.ClsServices.70]
Bereitstellung der dem CLS via "clsId" zugeordneten aktuellen Tarifinformationen und -stufen	Das SMGW **MUSS** ▸FA.ReadTariffState für das CLS umsetzen. [REQ.FAKAT.ClsServices.90]
Löschen von Session-Schlüsseln (Logout), so dass eine erneute Authentifizierung gegenüber dem SMGW erforderlich wird	Das SMGW **KANN** ▸FA.DoLogout für das CLS umsetzen. (▸ICS.FAKAT.ClsServices.10) [REQ.FAKAT.ClsServices.100] [6]
Geräte-Software- und Hardwareinformationen bereitstellen	Das SMGW **KANN** ▸FA.ReadDeviceInfo für das CLS umsetzen. (▸ICS.FAKAT.ClsServices.10) [REQ.FAKAT.ClsServices.110]
Auflistung der dem CLS zugeordneten FAs und Ressourcen	Das SMGW **SOLL** ▸FA.ListSmgwResources für das CLS umsetzen. (▸ICS.FAKAT.ClsServices.10) [REQ.FAKAT.ClsServices.150]

Tabelle 3.26 Übersicht der FA der Kategorie FAKAT.ClsServices

ICS



ICS.FAKAT.ClsServices.10

Der GWH **MUSS** im ICS deklarieren, welche MUSS+/SOLL/KANN FAs das SMGW für die Rolle CLS unterstützt.

[6] Ausloggen bezeichnet das Beenden einer Authentifizierung des Nutzers auf Anwendungs- oder Transportsicherungsebene, so dass die in der TLS-Verbindung vereinbarten, gemeinsame Sitzungsschlüssel auf Anwendungs- oder Transportsicherungsebene nicht mehr verwendet werden können.

ICS.FAKAT.ClsServices.30

Der GWH **MUSS** im ICS deklarieren, wie viele TLS-Proxy-Kanäle mit jeweils einer WKS.TLSPROXY- und zugeordneter HKS.TLSPROXY-Verbindung das SMGW gleichzeitig unterstützt.

3.7.3 Datenstrukturen der FA-Kategorie

Die Datenstruktur für den Export des erzeugten CLS-Schlüssels und CLS-Zertifikates wird in ▸Abschnitt 3.22.10 beschrieben.

3.7.4 FA.RequestProxyChByCls

3.7.4.1 Beschreibung

Nach Empfang einer Verbindungsaufbauanforderung eines über CLS_HAN_TLS_CRT identifizierten CLS, prüft das SMGW die als Aufrufparameter übergebene Identifikation[7] des Proxy-Kommunikationsprofiles (Siehe ▸Proxy-Kommunikationsprofil).

Nach erfolgreichem lokalen TLS-Verbindungsaufbau initiiert das SMGW die TLS-Verbindung zum EMT im WAN unter Berücksichtigung der Kommunikationsparameter des über das Proxy-Kommunikationsprofil referenzierten WAN-Kommunikationsprofils.

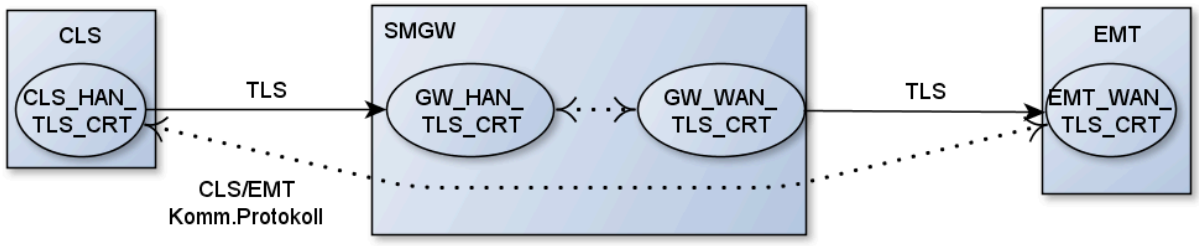


Abbildung 3.14. Transparenter Kommunikationskanal initiiert durch CLS

3.7.4.2 Auslöser

REQ.FA.RequestProxyChByCls.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer TLS-SNI-Anforderung über ▸HKS.TLSPROXY.SRV in der Rolle CLS.
- Empfang einer CONNECT-Anforderung über ▸HKS.TLSPROXY.SOCKS in der Rolle CLS.

▸ [FNN.20017.0]

3.7.4.3 Anforderungen

- (▸hanPeerRef "hks" gleich "TLSPROXY.SOCKS" und SOCKS-CONNECT mit IP-Adresse) Das SMGW **MUSS** das aktive Proxy-Kommunikationsprofil wählen, dessen ▸wanPeerRef "peerAddresses" die im CONNECT übermittelte IP-Adresse enthält. [REQ.FA.RequestProxyChByCls.30]
- (▸hanPeerRef "hks" gleich "TLSPROXY.SOCKS" und SOCKS-CONNECT mit Domain-Namen) Das SMGW **MUSS** das aktive Proxy-Kommunikationsprofil wählen, dessen ▸localServerName bzw. - wenn dieser nicht vorhanden ist - der ▸profileId im CONNECT übermittelten Domain-Namen entspricht. [REQ.FA.RequestProxyChByCls.40]
- (▸hanPeerRef "hks" gleich "TLSPROXY.SRV") Das SMGW **MUSS** das aktive Proxy-Kommunikationsprofil wählen, dessen ▸localServerName bzw. - wenn dieser nicht vorhanden ist - der ▸profileId dem TLS-SNI entspricht. [REQ.FA.RequestProxyChByCls.50]

[7] Bei HKS.TLSPROXY.SRV im TLS-SNI übermittelt, bei HKS.TLSPROXY.SOCKS im CONNECT-Parameter übermittelt

- Das SMGW **MUSS** die Verbindung zum EMT mit den WAN-Kommunikationsparametern des über ▸wanPeerRef zugeordneten Kommunikationsprofils initiieren. ▸ [FNN.20017.0] ▸ [FNN.20017.1] [REQ.WAN.Kommunikationsszenarien.100]
- Sofern die über ▸wanPeerRef zugeordnete TLS-Verbindung zum EMT nach allen Wiederholversuchen nicht aufgebaut werden konnte **MUSS** das SMGW die über ▸hanPeerRef zugeordnete TLS-Verbindung zum CLS beenden. [REQ.FA.RequestProxyChByCls.20]
- Das SMGW **MUSS** den Proxy-Verbindungstatus in ▸channelStatus und im zugehörigen ▸Status einer Proxy-Verbindung aktualisieren (▸ICS.FAKAT.ClsServices.10). ▸ [BSI.20018.0] ▸ [FNN.20018.1] [REQ.FA.RequestProxyChByCls.60]

3.7.5 FA.DoRequestProxyCh

3.7.5.1 Beschreibung

Dieser Anwendungsfall ermöglicht dem GWA, z.B. nach Auftrag vom EMT, das SMGW anzuweisen einen Proxy-Kommunikationskanal zwischen CLS und EMT ad-hoc oder zeitgesteuert herstellen zu lassen.

Dabei ist alternativ auch der regelmäßige Verbindungsaufbau über einen im ▸Abschnitt 3.22.37 definierten Parameter möglich.

3.7.5.2 Auslöser



REQ.FA.RequestProxyCh.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anforderung mit Identifikation des Proxy-Kommunikationsprofiles über ▸WKS.MANAGEMENT.
- Systemzeit des SMGW erreicht den im Proxy-Kommunikationsprofil spezifizierten "Proxy-Start Zeitpunkt" (▸triggerTime), sofern dieses Datenfeld in einem Proxy-Kommunikationsprofil konfiguriert ist.

▸ [FNN.20017.0]

3.7.5.3 Anforderungen

- Das SMGW **MUSS** den Proxy-Kanalaufbau ablehnen, sofern für den Aufrufparameter kein Proxy-Kommunikationsprofil mit dieser ▸profileId im SMGW konfiguriert ist. [REQ.HAN.HKS4.30]
- Das SMGW **MUSS** die Kommunikationsparameter des über ▸wanPeerRef referenzierten WAN-Kommunikationsprofils für die Kommunikation mit dem EMT verwenden. [REQ.HAN.HKS4.10]
- Das SMGW **MUSS** das Kommunikationsszenario ▸HKS.TLSPROXY.CLI und die Kommunikationsparameter des über ▸hanPeerRef referenzierten HAN-Kommunikationsprofils für die Kommunikation mit dem CLS verwenden. [REQ.FA.RequestProxyCh.20]
- Das SMGW **MUSS** den Proxy-Verbindungstatus in ▸channelStatus und im zugehörigen ▸Status einer Proxy-Verbindung beim Statuswechsel der WAN- oder HAN-TLS-Verbindung aktualisieren. [REQ.FA.RequestProxyCh.30]
- Das SMGW **MUSS** die über ▸wanPeerRef zugeordnete WAN-Verbindung initiieren, nachdem die HAN-TLS-Verbindung zum CLS erfolgreich aufgebaut ist. ▸ [FNN.20018.1] [REQ.FA.RequestProxyCh.40]
- Sofern die WAN-TLS-Verbindung zum EMT nach allen Wiederholversuchen nicht aufgebaut werden konnte, **MUSS** das SMGW die über ▸hanPeerRef zugeordnete lokale TLS-Verbindung zum CLS beenden. ▸ [BSI.20018.0] ▸ [FNN.20018.2] [REQ.FA.RequestProxyCh.50]

3.7.6 FA.DoCloseProxyCh

3.7.6.1 Beschreibung

Eine bestehende Proxy-Kommunikationsverbindung zwischen CLS und EMT wird unmittelbar beendet.

Ein Aufrufparameter identifiziert die zu beendende Verbindung anhand des ihr zugeordneten eindeutig identifizierten Proxy-Kommunikationsprofiles.

Der Abbau der Proxy-Kommunikationsverbindung zwischen CLS und EMT kann - abhängig von der Priorität ▸channelPrio - automatisch durch das SMGW ausgelöst werden, sofern die Anzahl der im SMGW möglichen TLS-Verbindungen überschritten würde.

3.7.6.2 Auslöser



REQ.FA.CloseProxyCh.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

▸ [FNN.20019.0]



REQ.FA.CloseProxyCh.12

Das SMGW **SOLL** diesen FA bei folgenden Ereignissen auslösen:

- (▸ICS.FA.CloseProxyCh.10) Die Zahl der gemäß ▸ICS.FAKAT.ClsServices.30 gleichzeitig bestehenden TLS-Proxy-Kommunikationskanäle ist erreicht und eine gemäß ▸channelPrio höher priorisierte TLS-Proxy-Kommunikationsverbindung soll aufgebaut werden.

▸ [FNN.20019.0]

3.7.6.3 Anforderungen

Das SMGW **MUSS** den Verbindungsabbau der über ▸hanPeerRef zugeordneten Verbindung zum CLS und der über ▸wanPeerRef zugeordneten Verbindung zum EMT innerhalb von 10s initiieren. ▸ [BSI.20020.0] ▸ [FNN.20020.1] [REQ.FA.CloseProxyCh.20]

ICS



ICS.FA.CloseProxyCh.10

Der GWH **MUSS** im ICS deklarieren, ob das SMGW die Kanal-Priorität im Proxy-Kommunikationsprofil für den Abbau der Verbindungen bei Erreichen der Maximalzahl gemäß ▸ICS.FAKAT.ClsServices.30 berücksichtigt.

3.7.6.4 Implementierungshinweis

Sofern mehrere Verbindungen gleicher Priorität bestehen und eine davon abgebaut werden muss, wird die mit der größten Verbindungsdauer gewählt.

3.7.7 FA.ReadProxyChStatus

3.7.7.1 Beschreibung

Stellt den Zustand eines über den Aufrufparameter identifizierten Proxy-Kommunikationskanals gemäß ▸Status einer Proxy-Verbindung bereit. Die Berechtigung und Zuordnung zum individuellen Proxy-Kommunikationsprofil ist mit der Authentifizierung des Auslösers des FA verknüpft. Ein authentifiziertes CLS kann nur für die ihm zugeordneten Proxy-Kommunikationskanäle den Status abrufen.

3.7.7.2 Auslöser



REQ.FA.ReadProxyChStatus.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle CLS.

3.7.7.3 Anforderungen

- (Aufruf über ▸HKS.WS1) Das SMGW **MUSS** die Anfrage ablehnen, wenn das für die TLS-Authentifizierung in ▸HKS.WS1 verwendete Zertifikat nicht dem CLS_HAN_TLS_CRT Zertifikat ▸peerCert aus dem HAN-Kommunikationsprofil des über ▸hanPeerRef des über den Aufrufparameter identifizierten Proxy-Kommunikationsprofils entspricht. [REQ.FA.ReadProxyChStatus.20]
- Das SMGW **MUSS** den Zustand ▸localConnectionState und ▸wanConnectionState entsprechend ihrer Bedeutung für den HAN- und WAN-Verbindungszustand setzen. [REQ.FA.ReadProxyChStatus.40]
- Das SMGW **MUSS** den Zustand ▸established gleich "true" setzen, wenn sowohl ▸localConnectionState als auch ▸wanConnectionState gleich "CONNECTED" sind und anderenfalls das Datenfeld auf "false" setzen. [REQ.FA.ReadProxyChStatus.30]
- Das SMGW **MUSS** dem Aufrufer den Proxy-Verbindungszustand gemäß ▸Status einer Proxy-Verbindung übermitteln. [REQ.FA.ReadProxyChStatus.50]

3.7.8 FA.DoCreateKeyPairAndClsCert

3.7.8.1 Beschreibung

Das SMGW erzeugt - mit dem Zufallszahlengenerator des Sicherheitsmodules des SMGW - ein Schlüsselpaar und ein mit dem privaten Schlüssel selbstsigniertes CLS_HAN_TLS_CRT$_{n+1}$.

Die Attribute des CLS-Zertifikates bestimmen sich nach [DS] Kapitel "HAN-Zertifikatsprofile", mit der CLS-ID des Client-Zertifikates der TLS-Verbindung, über die das SMGW die Anfrage erhält.

Privater Schlüssel und Zertifikat werden über die mit dem bisherigen CLS_HAN_TLS_CRT$_n$ authentisch verschlüsselte TLS-Verbindung an das CLS übermittelt.

Nachdem ein erfolgreicher TLS-Verbindungsaufbau mit dem neuen Zertifikat erfolgt ist, ersetzt das SMGW das bisherige Zertifikat CLS_HAN_TLS_CRT$_n$ in allen Proxy- und HAN-Kommunikationsprofilen.

3.7.8.2 Auslöser



REQ.FA.DoCreateKeyPairAndClsCert.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸HKS.WS1.

3.7.8.3 Anforderungen

- Das SMGW **MUSS** ein Schlüsselpaar für das CLS erzeugen und - sofern vorhanden - den Aufrufparameter (▸Parametersatz für Schlüssel- und Zertifikats-Erzeugung) berücksichtigen. [REQ.FA.DoCreateKeyPairAndClsCert.20]
- Das SMGW **MUSS** das Schlüsselpaar und das TLS-Zertifikat für das CLS gemäß [DS] Kapitel "HAN-Zertifikatsprofile" erzeugen. ▸ [BSI.5004.1] [REQ.FA.DoCreateKeyPairAndClsCert.30]
- Das SMGW **MUSS** die CLS-ID im *SubjectCN* des erzeugten TLS-Zertifikates identisch zum *SubjectCN* und die Sequenznummer im *SubjectDN* des erzeugten TLS-Zertifikates gegenüber dem zur Authentifizierung im aufrufenden Kommunikationsszenario verwendeten TLS-Client-Zertifikates um eins erhöhen. Sofern kein gültiger SubjectCN oder keine gültige Sequenznummer ermittelt werden kann, wird als SubjectCN die CLS-ID aus ▸userId und die Sequenznummer "1" eingesetzt. [REQ.FA.DoCreateKeyPairAndClsCert.31]
- Das SMGW **MUSS** das Schlüsselpaar und Zertifikat (▸Abschnitt 3.22.10) an den Aufrufer übermitteln. ▸ [BSI.5004.2] ▸ [BSI.5004.0] [REQ.FA.DoCreateKeyPairAndClsCert.40]
- Nach der nächsten erfolgreichen Authentifizierung des CLS mit CLS_HAN_TLS_CRT$_{n+1}$ **MUSS** das SMGW das CLS_HAN_TLS_CRT$_n$ im Datenfeld ▸peerCert aller HAN-Kommunikationsprofile durch CLS_HAN_TLS_CRT$_{n+1}$ ersetzen und persistieren. Das CLS_HAN_TLS_CRT$_n$ wird nicht mehr verwendet. [REQ.FA.DoCreateKeyPairAndClsCert.50]

3.7.8.4 Implementierungshinweise

Das EC-Schlüsselpaar wird gemäß [TR-03111] Kapitel "Elliptic Curve Key Pair Generation – ECKeyPair" mit dem einem Zufallszahlengenerator gemäß [TR-03109-3] erzeugt. Da das Schlüsselpaar an das CLS exportiert wird, wird das Schlüsselpaarobjekt nicht im Sicherheitsmodul erzeugt.

Das erzeugte Schlüsselpaar und das bisherige CLS_HAN_TLS_CRT$_n$ wird nach Persistierung in den Kommunikationsprofilen nicht mehr vom SMGW benötigt und soll gelöscht werden.

Solange das CLS_HAN_TLS_CRT$_{n+1}$ noch nicht im Kommunikationsprofil persistiert wurde, wird bei einem erneuten Aufruf des FA die Sequenznummer nicht erhöht, da das zur Authentifizierung verwendete TLS-Client-Zertifikat CLS_HAN_TLS_n weiterhin die nicht inkrementierte Sequenznummer erhält. Ein neues Schlüsselpaar kann in diesem Fall erzeugt werden.

3.8 Dienste für den Servicetechniker im HAN (FAKAT.SrvServices)

3.8.1 Übersicht

Anwendungsfälle dieser Kategorie (bisher HAF2, HAF4, HAF5) ermöglichen einem Servicetechniker im HAN die Diagnose und Behebung von Kommunikationsstörungen im WAN, um die Kommunikation mit dem GWA wiederherzustellen.

Wird innerhalb dieser FA-Kategorie von *einem* oder *dem* Servicetechniker gesprochen, ist ein über ein TLS-Zertifikat authentifizierter Servicetechniker gemeint, dessen Berechtigung durch den GWA zuvor im SMGW parametriert wurde.

Das SMGW realisiert die FA gemäß ▸Tabelle 3.27. Die FA sind z.B. in ▸FAKAT.SmgwAdministration beschrieben.

3.8.2 Übersicht der FA

Aufgabe	Umsetzung
Bereitstellung des System-Logs zur Diagnose von Verbindungsproblemen (bisher HAF2)	Das SMGW **MUSS** ▸FA.ExportSysLog für den SRV umsetzen. [REQ.HAN.ServiceTechnikerDatenbereitstellung.10]
Bereitstellung des Eich-Logs	Das SMGW **SOLL** ▸FA.ExportCalLog für den SRV umsetzen.(▸ICS.FAKAT.SrvServices.200) [REQ.FAKAT.SrvServices.170]
Bereitstellung des Status von Netzwerkschnittstellen zur Diagnose von Verbindungsproblemen	Das SMGW **SOLL** ▸FA.ReadNetworkIfStatus für den SRV umsetzen. (▸ICS.FAKAT.SrvServices.200) [REQ.HAN.ServiceTechnikerDatenbereitstellung.20]
Ermittlung der Dienst- und Kommunikationsadressen zur Ausführung von Anwendungsfällen des Servicetechnikers (bisher HAF2)	Das SMGW **SOLL** ▸FA.ListSmgwResources für den SRV umsetzen. (▸ICS.FAKAT.SrvServices.200) [REQ.HAN.ServiceTechnikerDatenbereitstellung.30]
Selbsttest durch Servicetechniker auslösen (bisher HAF5)	Das SMGW **MUSS** ▸FA.DoSelftest für den SRV umsetzen. [REQ.HAN.ServiceTechnikerSelbsttest.10]
Ändern der Kommunikationsparameter zum Wiederherstellen der Transportverbindung zum GWA (bisher HAF4)	Das SMGW **SOLL** ▸FA.UpdateWanComProfile für den SRV umsetzen. (▸ICS.FAKAT.SrvServices.200) [REQ.HAN.ServiceTechnikerGwaKommunikation.10] [8]
Ändern der WAN-Schnittstellen-Konfiguration zum Wiederherstellen der WAN-Kommunikation durch den Servicetechniker (bisher HAF4)	Das SMGW **SOLL** ▸FA.UpdateWanIfProfile für den SRV umsetzen. (▸ICS.FAKAT.SrvServices.200) [REQ.FAKAT.SrvServices.10]

[8] Es dürfen nur bestimmte Parameter, wie z.B. die IP-Adresse des Kommunikationssystems oder Timeout-Parameter geändert werden um die Kommunikation mit dem GWA wieder herzustellen. Zertifikate können nicht verändert werden.

Aufgabe	Umsetzung
Auslesen der WAN-Schnittstellenkonfiguration durch den Servicetechniker	Das SMGW **SOLL** ▸FA.ReadWanIfProfile für den SRV umsetzen. (▸ICS.FAKAT.SrvServices.200) [REQ.HAN.ServiceTechnikerGwaKommunikation.20]
Auslesen der HAN-Schnittstellenkonfiguration durch den Servicetechniker	Das SMGW **SOLL** ▸FA.ReadHanIfProfile für den SRV umsetzen. (▸ICS.FAKAT.SrvServices.200) [REQ.FAKAT.SrvServices.120]
Auslesen der LMN-Schnittstellenkonfiguration durch den Servicetechniker	Das SMGW **SOLL** ▸FA.ReadLmnIfProfile für den SRV umsetzen. (▸ICS.FAKAT.SrvServices.200) [REQ.FAKAT.SrvServices.130]
Auslesen eines GWA-WAN-Kommunikationsprofiles	Das SMGW **SOLL** ▸FA.ReadWanComProfile für den SRV umsetzen. (▸ICS.FAKAT.SrvServices.200) [REQ.FAKAT.SrvServices.20]
Auslesen eines LMN-Kommunikationsprofiles	Das SMGW **SOLL** ▸FA.ReadLmnComProfile für den SRV umsetzen. (▸ICS.FAKAT.SrvServices.200) [REQ.FAKAT.SrvServices.60]
Auslesen eines HAN-Kommunikationsprofiles	Das SMGW **SOLL** ▸FA.ReadHanComProfile für den SRV umsetzen. (▸ICS.FAKAT.SrvServices.200) [REQ.FAKAT.SrvServices.70]
Auslesen eines Proxy-Kommunikationsprofiles durch den Servicetechniker	Das SMGW **SOLL** ▸FA.ReadProxyComProfile für den SRV umsetzen. (▸ICS.FAKAT.SrvServices.200) [REQ.FAKAT.SrvServices.80]
Status der Zeitführung durch Servicetechniker auslesen	Das SMGW **SOLL** ▸FA.ReadTimeSyncStatus für den SRV umsetzen (▸ICS.FAKAT.SrvServices.200) [REQ.FAKAT.SrvServices.30]
Auslesen der im SMGW gespeicherten (RootCA-)Zertifikate durch den Servicetechniker	Das SMGW **SOLL** ▸FA.ReadCertificate für den SRV umsetzen. (▸ICS.FAKAT.SrvServices.200) [REQ.FAKAT.SrvServices.40]
Nutzerdatenbereinigung durch den Servicetechniker auslösen	Das SMGW **MUSS+** ▸FA.DoDeleteUserData für den SRV umsetzen. (▸ICS.FAKAT.SrvServices.200) [REQ.FAKAT.SrvServices.50]
Liste der vom SMGW identifizierten Messeinrichtungen an den Servicetechniker exportieren	Das SMGW **SOLL** ▸FA.ListIdentifiedMeters für den SRV umsetzen. (▸ICS.FAKAT.SrvServices.200) [REQ.FAKAT.SrvServices.90]
Geräte-Software- und Hardwareinformationen bereitstellen	Das SMGW **SOLL** ▸FA.ReadDeviceInfo für den SRV umsetzen.(▸ICS.FAKAT.SrvServices.200) [REQ.FAKAT.SrvServices.100]
Gerätestatus bereitstellen (SMGW, Messeinrichtung)	Das SMGW **SOLL** ▸FA.ReadDeviceStatus für den SRV umsetzen.(▸ICS.FAKAT.SrvServices.200) [REQ.FAKAT.SrvServices.190]
Neustart zum Erreichen der operativen/administrativen Betriebsbereitschaft auslösen	Das SMGW **MUSS** ▸FA.DoReboot für den SRV umsetzen.(▸ICS.FAKAT.SrvServices.200) [REQ.FAKAT.SrvServices.110]
Löschen von Session-Schlüsseln (Logout), so dass eine erneute Authentifizierung gegenüber dem SMGW erforderlich wird	Das SMGW **SOLL** ▸FA.DoLogout für den SRV umsetzen.(▸ICS.FAKAT.SrvServices.200) [REQ.HAN.SicherungKommunikationConSrv.21] [9]
Systemzeit zur Synchronisation bereitstellen	Das SMGW **SOLL** ▸FA.NtpTimeService für den SRV umsetzen. (▸ICS.FAKAT.SrvServices.200) [REQ.FAKAT.SrvServices.140]
Kommunikative Anbindung im Zähler über das SMGW aufheben (Crypto-Reset)	Das SMGW **SOLL** ▸FA.DoRemoveSmgwAssocInMtr für den SRV umsetzen. (▸ICS.FAKAT.SrvServices.200) [REQ.FAKAT.SrvServices.150]
Älteste Eichlog-Einträge verkürzen	Das SMGW **SOLL** ▸FA.DoTruncateCalLog für den SRV umsetzen. (▸ICS.FAKAT.SrvServices.200) [REQ.FAKAT.SrvServices.160]
CLS im HAN auflisten	Das SMGW **SOLL** ▸FA.ListIdentifiedCls für den SRV umsetzen. (▸ICS.FAKAT.SrvServices.200) [REQ.FAKAT.SrvServices.180]

Tabelle 3.27 Übersicht der FA der Kategorie FAKAT.SrvServices

ICS

[9] Ausloggen bezeichnet das Beenden einer Authentifizierung des Nutzers auf Anwendungs- oder Transportsicherungsebene, so dass die in der TLS-Verbindung vereinbarten, gemeinsame Sitzungsschlüssel auf Anwendungs- oder Transportsicherungsebene nicht mehr verwendet werden können.



ICS.FAKAT.SrvServices.200

Der GWH **MUSS** im ICS deklarieren, welche MUSS+/SOLL/KANN FAs das SMGW für den SRV umsetzt.

3.9 Erweiterte Dienste für Messeinrichtungen im LMN (FAKAT.MtrServices)

3.9.1 Übersicht

Anwendungsfälle dieser Kategorie ermöglichen die Nutzung von Diensten des SMGW durch die Messeinrichtung bzw. der Messeinrichtung durch das SMGW, die über die kommunikative Anbindung (siehe ▸FAKAT.LmnComConfig) und Messdatenbereitstellung (siehe ▸FAKAT.ValCapture) hinausgehenden. Die Nutzung der Dienste setzt eine Messeinrichtung mit entsprechenden Fähigkeiten voraus.

Das SMGW realisiert die FA gemäß ▸Übersicht der FA der Kategorie FAKAT.MtrServices.

3.9.2 Übersicht der FA

Aufgabe	Umsetzung
Übermittlung von Messgeräte-Informationen an das SMGW	Das SMGW **SOLL** ▸FA.RetrieveDeviceInfoFromMtr umsetzen. (▸ICS.FAKAT.MtrServices.10) [REQ.FAKAT.MtrServices.10]
Übermittlung der Systemzeit des SMGW an die Messeinrichtung	Das SMGW **MUSS+** ▸FA.ExportTimeToMtr umsetzen. (▸ICS.FAKAT.MtrServices.10) [REQ.FAKAT.MtrServices.20]
Übermittlung einer (Firmware-)Datei vom SMGW an die Messeinrichtung	Das SMGW **MUSS+** ▸FA.ExportFileToMtr umsetzen. (▸ICS.FAKAT.MtrServices.10) [REQ.FAKAT.MtrServices.30]
Aufheben der Kommunikativen SMGW-Anbindung in der Messeinrichtung	Das SMGW **SOLL** ▸FA.DoRemoveSmgwAssocInMtr für den GWA umsetzen. (▸ICS.FAKAT.MtrServices.10) [REQ.LMN.Zaehlerverwaltung.60]
Zurücksetzen des Manipulationszustandes einer Messeinrichtung	Das SMGW **KANN** ▸FA.DoResetTamperState für den GWA umsetzen. (▸ICS.FAKAT.MtrServices.10) [REQ.FAKAT.MtrServices.40]
Abfrage des Uhrenzustandes von der Messeinrichtung	Das SMGW **MUSS+** ▸FA.RetrieveClockStateFromMtr umsetzen. (▸ICS.FAKAT.MtrServices.10) [REQ.FAKAT.MtrServices.50]
Abruf eines Logs oder einer Datei von der Messeinrichtung	Das SMGW **SOLL** ▸FA.RetrieveFileFromMtr umsetzen. (▸ICS.FAKAT.MtrServices.10) [REQ.FAKAT.MtrServices.60]
Auslösen einer Aktualisierung der Firmware einer angebundenen Messeinrichtung	Siehe ▸FAKAT.SmgwFwUpdate
Zertifikatserneuerung der Messeinrichtung	Siehe ▸FAKAT.LmnComConfig

Tabelle 3.28 Übersicht der FA der Kategorie FAKAT.MtrServices

ICS



ICS.FAKAT.MtrServices.10

Der GWH **MUSS** im ICS deklarieren, welche MUSS+/SOLL/KANN FAs das SMGW für Messeinrichtungen an der LMN-Schnittstelle umsetzt.

3.9.3 FA.ExportTimeToMtr

3.9.3.1 Beschreibung

Das SMGW exportiert die aktuelle - mit der gesetzlichen Zeit synchronisierte - Systemzeit authentisch an eine über den Aufrufparameter identifizierte Messeinrichtung. Damit hat die Messeinrichtung die Möglichkeit die Zeitabweichung zwischen Systemzeit und gesetzlicher Zeit zu bestimmen und die Messgeräteuhr zu synchronisieren.

Die mit der gesetzlichen Zeit synchronisierte Messgeräteuhrzeit kann zur Registrierung von Messwerten in der Messeinrichtung zur Verwendung im geschäftlichen Verkehr verwendet werden.

Dieser Anwendungsfall erfordert eine bidirektionale Kommunikation zwischen Zähler und SMGW.

3.9.3.2 Auslöser



REQ.FA.ExportTimeToMtr.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- (Für jedes LMN-Kommunikationsprofil vom Typ ▸LKS1 das aus einem Auswertungsprofil vom Typ "TAF15" referenziert wird) Periodisch einmal in 24 Stunden

3.9.3.3 Anforderungen

Das SMGW **MUSS** die Systemzeit, Informationen zum Zeitoffset zwischen UTC und lokaler Zeit und die Informationen zur Bestimmung der Abweichung von der gesetzlichen Zeit gemäß [DS] Kapitel "SML" über ▸LKS1 an die Messeinrichtung übermitteln. [REQ.FA.ExportTimeToMtr.20]

3.9.4 FA.ExportFileToMtr

3.9.4.1 Beschreibung

Das SMGW übermittelt eine Datei an die Messeinrichtung. Die Datei kann Firmwareupdates oder Konfigurationsparameter für die Messeinrichtung oder deren Kommunikationsadapter enthalten.

Die interne Dateistruktur ist für das SMGW transparent, somit kann das SMGW keine Prüfung der Inhalte übernehmen oder Interoperabilität bzgl. der Inhalte gewährleisten. Die Datei wurde zuvor vom GWA in das SMGW importiert.

Die Endpunkt-Adresse der Datei im Zähler und die Messgeräte-Identifikation werden über ein zuvor konfiguriertes ▸Firmware-Update-Profil bestimmt.

Durch ▸FA.UpdateFwUpdateConfig ist gewährleistet, dass ein ▸Firmware-Update-Profil nur für Messeinrichtungen mit der Fähigkeit zum Dateiempfang konfiguriert werden können.

Dieser Anwendungsfall erfordert eine bidirektionale Kommunikation zwischen Zähler und SMGW.

Nach positiver Bestätigung der Annahme der Datei durch die Messeinrichtung wird das zugeordnete ▸Firmware-Update-Profil vom SMGW gelöscht.

3.9.4.2 Auslöser



REQ.FA.ExportFileToMtr.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Für jede Auslösebedingung eines FwUpdateProfiles (siehe ▸timeOfActivation), dessen ▸deviceId eine Messeinrichtung bezeichnet.

3.9.4.3 Anforderungen

- Das SMGW **MUSS** die im Firmware-Updateprofil bezeichnete, im SMGW gespeicherte Datei gemäß [DS] Kapitel "SML - Smart Message Language" über ▸LKS1 an die im ▸Firmware-Update-Profil konfigurierte Endpunkt-Adresse der Messeinrichtung übermitteln. ▸ [BSI.1016.1] ▸ [BSI.1016.0] [REQ.FA.ExportFileToMtr.20]
- Nach erfolgreicher Übermittlung (und Aktivierung durch die Messeinrichtung) **MUSS** das SMGW das auslösende ▸Firmware-Update-Profil und die persistierte Datei im SMGW löschen (siehe ▸FA.DeleteFwUpdateConfig). [REQ.FA.ExportFileToMtr.30]

3.9.4.4 Implementierungshinweise

Die Messeinrichtung teilt dem SMGW mit, wenn die Übertragung nicht erfolgreich ist. Bei ausbleibender Bestätigung der Messeinrichtung, z.B. bei Übertragungsfehlern sollte eine Nachrichten-Wiederholung auf Transportebene durchgeführt werden.

3.9.5 FA.RetrieveDeviceInfoFromMtr

3.9.5.1 Beschreibung

Das SMGW ruft von der über den Aufrufparameter identifizierten Messeinrichtung Geräte-Statusinformationen ab und stellt sie dem Aufrufer bereit.

Die Informationen werden für die Durchführung der Anwendungsfälle in ▸FAKAT.MtrServices und ▸FAKAT.ValCapture durch den GWA benötigt.

Dieser Anwendungsfall erfordert eine bidirektionale Verbindung zwischen Zähler und SMGW.

3.9.5.2 Auslöser

REQ.FA.ReadDeviceInfoFromMtr.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Aufruf von ▸FA.ReadDeviceInfo empfangen.

3.9.5.3 Anforderungen

- Das SMGW **MUSS** die Software-Version, Kennzeichnung des Hardware/Firmware-Typs gemäß [DS] Kapitel "SML" über ▸LKS1 von der Messeinrichtung anfordern. [REQ.FA.ReadDeviceInfoFromMtr.20]
- Das SMGW **MUSS** die von der Messeinrichtung über ▸LKS1 empfangenen Geräteinformationen gemäß ▸Device-Info an den Aufrufer übermitteln. [REQ.FA.ReadDeviceInfoFromMtr.30]

3.9.6 FA.DoRemoveSmgwAssocInMtr

3.9.6.1 Beschreibung

Das SMGW übermittelt eine Anweisung zum Aufheben des Pairings mit dem SMGW an die im Aufrufparameter identifizierte Messeinrichtung.

Sofern ein PSK für das Pairing genutzt wird (LKS1.PSK), verwendet die Messeinrichtung anschließend den initialen, vom Hersteller der Messeinrichtung vergebenen Master Key (MK_0) für ein erneutes Pairing.

Sofern ein initiales TLS-Zertifikat für das Pairing genutzt wird, verwendet die Messeinrichtung anschließend das vom Hersteller der Messeinrichtung erzeugte $MTR_LMN_TLS_CRT_0$ für ein erneutes Pairing.

Sofern das GW_LMN_TLS_CRT in der Messeinrichtung für die Authentifizierung des SMGW persistiert ("gepinnt") wurde, wird dieses Pinning aufgehoben, so dass die Messeinrichtung künftig einem anderen SMGW vertrauen kann.

Vorbedingungen sind: Das LMN-Kommunikationsprofil mit dem initialen PSK für die Messeinrichtung liegt im SMGW vor und kein aktives Auswertungsprofil verweist auf die identifizierte Messeinrichtung.

Nach erfolgreicher Ausführung ist der Zähler nicht mehr kommunikativ mit diesem SMGW verbunden. Eine erneute initiale kommunikative Anbindung (siehe ▸FA.DoInitialMtrSmgwPairing) ist möglich.

Hinweis: Das LMN-Kommunikationsprofil wird nicht gelöscht.

Dieser Anwendungsfall wird auch als "Crypto-Reset" bezeichnet.

3.9.6.2 Auslöser

REQ.FA.DoRemoveSmgwAssocInMtr.30

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle SRV.

3.9.6.3 Anforderungen

- Das SMGW **MUSS** die Anforderung ablehnen, wenn kein LMN-Kommunikationsprofil für die im Aufrufparameter identifizierte Messeinrichtung aktiv ist. ▸[BSI.1010.2] [REQ.FA.DoRemoveSmgwAssocInMtr.10]

- Das SMGW **MUSS** die Anforderung ablehnen, wenn das LMN-Kommunikationsprofil einen unidirektional angebundenen Zähler (LKS2) referenziert. ▸ [BSI.1010.2] [REQ.FA.DoRemoveSmgwAssocInMtr.12]
- Das SMGW **MUSS** die Anforderung ablehnen, wenn kein ▸pairingKey (für LKS1.PSK) oder initiales ▸mtrTlsCert ($MTR_LMN_TLS_CRT_0$) für die im Aufrufparameter identifizierte Messeinrichtung konfiguriert ist. ▸ [BSI.1010.2] [REQ.FA.DoRemoveSmgwAssocInMtr.13]
- Das SMGW **MUSS** das Auflösen der Assoziation mit dem SMGW in der Messeinrichtung gemäß [DS] "Bidirektionale LMN-Kommunikation über HDLC" über ▸LKS1.PSK mit dem symmetrischen Schlüssel (▸pairingKey) aus dem LMN-Kommunikationsprofil der Messeinrichtung auslösen und nach positiver Bestätigung durch die Messeinrichtung das Datenfeld ▸smgwTlsCert und ▸mtrTlsCert im LMN-Kommunikationsprofil löschen. ▸ [FNN.1010.0] ▸ [FNN.1010.1] [REQ.FA.DoRemoveSmgwAssocInMtr.20]

3.9.7 FA.DoResetTamperState

3.9.7.1 Beschreibung

Der FA ermöglicht das Zurücksetzen eines in der Messeinrichtung erkannten Manipulationszustandes, wie z.B. Klemmdeckelöffnung oder magnetische Beeinflussung. Dieser Zustand kann sowohl beabsichtigt (bei der Installation) oder unbeabsichtigt auftreten. Der GWA oder Service-Techniker klärt die Ursache und ruft dann diesen FA auf.

Der Manipulationszustand des Klemmdeckels wird vom SMGW nicht als abrechnungsrelevanter Fehler eingestuft.

Der Aufruf dieses FA initiiert das Zurücksetzen aller Manipulationsbits.

Dies setzt voraus, das die Messeinrichtung die Fähigkeit zum Zurücksetzen der Manipulationserkennung hat und bidirektional mit dem SMGW kommunizieren kann.

3.9.7.2 Auslöser



REQ.FA.DoResetTamperState.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle SRV.

3.9.7.3 Anforderungen

- Das SMGW **MUSS** den Aufruf ablehnen sofern die Geräte-ID im Aufrufparameter keiner ▸meterId eines LMN-Kommunikationsprofils vom Typ "LKS1" entspricht. [REQ.FA.DoResetTamperState.20]
- Das SMGW MUSS das Zurücksetzen im Zähler gemäß [DS] Kapitel "SML" TA.SML.CLI.ResetTamperState ausführen und die Antwort vom Zähler im Syslog protokollieren. ▸ [BSI.19022.0] ▸ [BSI.19022.1] [REQ.FA.DoResetTamperState.30]

3.9.8 FA.RetrieveClockStateFromMtr

3.9.8.1 Beschreibung

Das SMGW ruft von der über den Aufrufparameter identifizierten Messeinrichtung die Zustandsinformationen der Geräteuhr und der Zeitsynchronisation ab und stellt sie dem Aufrufer bereit. Es findet durch das SMGW keine Korrektur von registrierten Messwerten statt.

Die Informationen werden für die Überwachung der korrekten Zeitführung zur Zeitstempelung von Messwerten in der Messeinrichtung durch den GWA benötigt.

Dieser Anwendungsfall erfordert eine bidirektionale Verbindung zwischen Messeinrichtung und SMGW (LKS1).

3.9.8.2 Auslöser



REQ.FA.RetrieveClockStateFromMtr.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Aufruf von ▸FA.ReadTimeSyncStatus für Messeinrichtung LKS1 empfangen.

3.9.8.3 Anforderungen

- Das SMGW **MUSS** den Uhrenzustand, die aktuelle Zeit und Abweichung zwischen UTC und lokaler Zeitzone und Informationen zur Zeitsynchronisation gemäß [DS] Kapitel "SML" über ▸LKS1 von der Messeinrichtung anfordern. [REQ.FA.RetrieveClockStateFromMtr.20]
- Das SMGW **MUSS** die von der Messeinrichtung über ▸LKS1 empfangenen Statusinformationen gemäß ▸Zeitsynchronisationsstatus an den Aufrufer übermitteln. [REQ.FA.RetrieveClockStateFromMtr.30]

3.9.9 FA.RetrieveFileFromMtr

3.9.9.1 Beschreibung

Das SMGW fragt eine im Aufrufparameter bestimmte Datei, optional eingegrenzt auf einen bestimmten Zeitraum von der im Aufrufparameter identifizierten Messeinrichtung an und speichert die von der Messeinrichtung empfangene Datei temporär, um sie nach Ende der Übertragung an den im Aufrufparameter benannten EMT zu versenden.

Die interne Struktur der Datensätze ist für das SMGW nicht bekannt, somit kann das SMGW keine Prüfung der Inhalte übernehmen oder Interoperabilität bzgl. der Inhalte gewährleisten. Die Datei kann protokollierte Ereignisse (z.B. Eichlog der Messeinrichtung) oder Messwertdatensätze beinhalten.

Nach erfolgreicher Übertragung der Datei kann der GWA die Datei aus dem SMGW mittels FA.ReadFile abrufen.

Dieser Anwendungsfall erfordert eine bidirektionale Verbindung zwischen Messeinrichtung und SMGW.

3.9.9.2 Auslöser



REQ.FA.RetrieveFileFromMtr.10

Das SMGW **MUSS** den FA bei folgenden Ereignissen auslösen:

- Anforderung über ▸WKS.MANAGEMENT empfangen.

3.9.9.3 Anforderungen

Das SMGW **MUSS** die im Aufrufparameter übergebene Identifikation der Datei und den Abfragezeitraum (von-bis, UTC), gemäß [DS] Kapitel "SML" über ▸LKS1 zur Abfrage an die Messeinrichtung übermitteln. [REQ.FA.RetrieveFileFromMtr.20]

Das SMGW **MUSS** die von der Messeinrichtung empfangenen Datensätze der Datei temporär speichern. [REQ.FA.RetrieveFileFromMtr.30]



ICS.FA.RetrieveFileFromMtr.20

Der GWH deklariert im ICS, welche maximale Dateigröße (in Kilobytes) die das SMGW empfangen und speichern kann.

3.10 Zeitführung des SMGW (FAKAT.SmgwTimeSync)

3.10.1 Übersicht

Das SMGW besitzt eine Systemuhr, die die Systemzeit für die Kommunikationsprotokolle, die Zertifikatsprüfung, die Registrierung von Messwerten, weitere Anwendungsfälle des SMGW und die lokalen mit dem SMGW kommunizierenden Geräte bereitstellt. Das SMGW synchronisiert die Systemzeit so mit einem Zeitserver des GWA (siehe ▸Synchronisations-Hierarchie des Intelligenten Messsystems), dass vorgegebene maximale Abweichungen von der gesetzlichen Zeit nicht überschritten werden. Dazu synchronisiert sich dieser Zeitserver

mit den Zeitservern der PTB, die die gesetzliche Zeit bereitstellen (siehe [TR-03109-6]). Durch die Synchronisation mit dem Zeitserver erhält das SMGW die Information über die Zeitabweichung der Systemzeit von der gesetzlichen Zeit und synchronisiert sich mit der gesetzlichen Zeit.

Der Zeitserver ist der GWA-Rolle zugeordnet.

Bezugszeitskala ist Universal Time Coordinated (UTC). Die Differenz zur lokalen Zeit (gesetzliche Zeit) entspricht den Vorgaben der [SoZV]. Bei Anpassung der Vorgaben kann der GWA die Konfiguration ändern. Protokollierte und aufgezeichnete Messwerten und Ereignisse enthalten eine Information über die Zeitdifferenz zwischen lokaler Zeit und UTC.

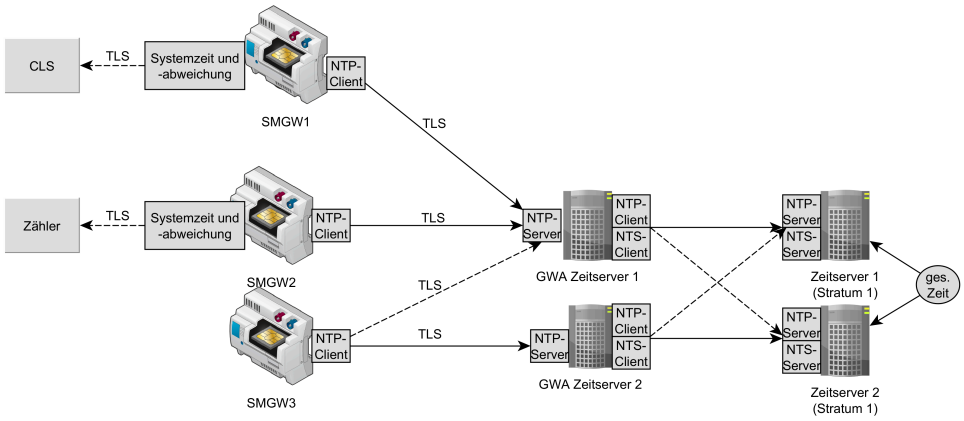


Abbildung 3.15. Synchronisations-Hierarchie des Intelligenten Messsystems

Die Anwendungsfälle dieser Kategorie beschreiben die Funktionalität zur Zeitsynchronisation des SMGW.

3.10.2 Übersicht der FA

Aufgabe	Umsetzung
Systemzeit mit Zeitserver des GWA synchronisieren	Das SMGW **MUSS** ▸FA.TimeSyncWithGwa umsetzen. [REQ.WAN.ZugriffAufGwa-Dienste.10]
Status der Zeitführung durch GWA auslesen	Das SMGW **SOLL** ▸FA.ReadTimeSyncStatus für den GWA umsetzen. [REQ.WAN.Management.272]
Auslösen der Zeitsynchronisation durch den GWA	Das SMGW **SOLL** ▸FA.TimeSyncWithGwa für den GWA umsetzen. [REQ.WAN.Management.273]

Tabelle 3.29 Übersicht der FA der Kategorie FAKAT.SmgwTimeSync

ICS

ICS.FAKAT.SmgwTimeSync.40

Der GWH **MUSS** im ICS angeben, welche FAs dieser FA-Kategorie mit Einstufung KANN, SOLL oder MUSS+ das SMGW für die Rolle GWA unterstützt.

3.10.3 Anforderungen

Sofern nach einem Neustart des SMGW keine Gangreserve vorhanden oder die "Gangreservedauer" (siehe ▸ICS.WAF2.Zeitsynchronisation.10>) überschritten wurde, **MUSS** das SMGW ▸timeValid gleich "false" setzen. ▸ [PTB.13001.1] [REQ.WAF2.Zeitsynchronisation.52]

3.10.4 Datenstrukturen

Die Datenstruktur für den Zeitsynchronisationsstatus ist in ▸Abschnitt 3.22.47 beschrieben.

3.10.5 FA.TimeSyncWithGwa

3.10.5.1 Beschreibung

Durch gerätespezifische Einflüsse (Umgebungstemperatur, Alterung, Fertigungstoleranz zeitbestimmender Bauelemente) entfernt sich die Systemzeit ohne Nachführung stetig in einer kleinen Rate von der gesetzlichen Zeit. Deshalb überwacht das SMGW die Zeit seit der letzten Zeitsynchronisation und führt mit diesem FA eine Zeitsynchronisation mit dem Zeitserver des GWA durch. Die aus der Zeitsynchronisation mit dem Zeitserver des GWA ermittelten Parameter werden zur Kompensation des Drift der Systemzeit verwendet.

Das SMGW verwendet ausschließlich das TLS-gesicherte NTP-Protokoll zur Zeitsynchronisation. Andere Technologien (wie bspw. DCF77) dürfen nicht verwendet werden.

Der Messbetrieb wird nach der ersten erfolgreichen Zeitsynchronisation mit dem GWA-Zeitserver nach Inbetriebnahme an der Messstelle aufgenommen.

Fehlerbetrachtung

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

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

Für eine Fehlerbetrachtung im Rahmen dieser Einsatzumgebung müsste das Fehlerkontingent sowohl der Strecke SMGW <--> GWA-Zeitserver als auch das der Strecke GWA-Zeitserver <--> PTB-Zeitserver betrachtet werden. Da die Zeitabweichung zwischen GWA-Zeitserver und PTB-Zeitserver auf 0,01 % der kleinsten Registrierperiode oder 90 ms begrenzt ist[10], wird davon ausgegangen, dass der gesamte Fehler durch die Strecke SMGW <--> GWA-Zeitserver dominiert wird. Damit wird im Folgenden für die Betrachtung des möglichen Fehlers nur die Strecke zwischen SMGW und GWA-Zeitserver betrachtet.

Eine vermutete zu große Abweichung der Systemzeit wird durch das SMGW bei anhaltend fehlgeschlagener Zeitsynchronisation angenommen. Dies wird im kombinierten Statuswort ▸Abschnitt 3.22.13 für die künftige Registrierung von Messwerten vermerkt und führt weiterhin zu einer Benachrichtigung des GWA.

Eine bei erfolgreicher Zeitsynchronisation erkannte Abweichung der Systemzeit von der gesetzlichen Zeit, die die 3 % Fehlergrenze zur kleinsten Registrierperiode (in der Regel 900 Sekunden) überschreitet, wird vom SMGW protokolliert und der GWA über dieses Ereignis informiert. Da der GWA-Zeitserver die gesetzliche Zeit bereitstellt, wird die Systemzeit in diesem Fall trotzdem gemäß der per Zeitsynchronisation gelieferten Zeit gestellt und die Systemzeit dann als valide angenommen.

Nach der nächsten erfolgreichen Zeitsynchronisation mit einer Abweichung von weniger als 3 % der Registrierperiodendauer zur gesetzlichen Zeit, wird die Systemzeit als gültig angenommen und erneut Messwerte zur Abrechnung gebildet.

Ablauf

▸Abbildung 3.16 stellt den durch die Anforderungen beschriebenen Ablauf einer einzelnen Zeitsynchronisation grafisch dar. Dieser Ablauf wird unabhängig vom Auslöser dieses FA durchgeführt.

Das SMGW kann optional über eine Gangreserve verfügen. Sofern die Gangreserve nach einem Neustart nicht erschöpft ist, kann das SMGW die Zeit auch vor der ersten erfolgreichen Zeitsynchronisation bereits als valide annehmen und den Messbetrieb wieder aufnehmen.

▸Abbildung 3.17 stellt den Status der Systemzeit beim Eintreten verschiedener Ereignisse beispielhaft dar.

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

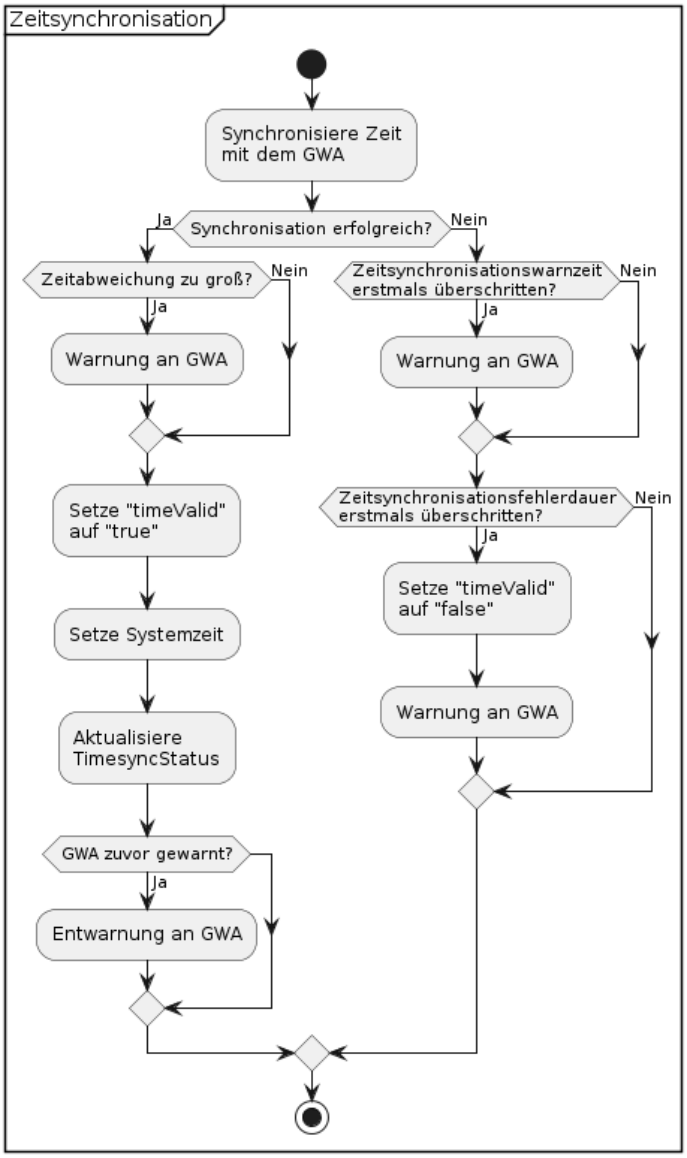


Abbildung 3.16. Ablaufdiagramm einer Zeitsynchronisation

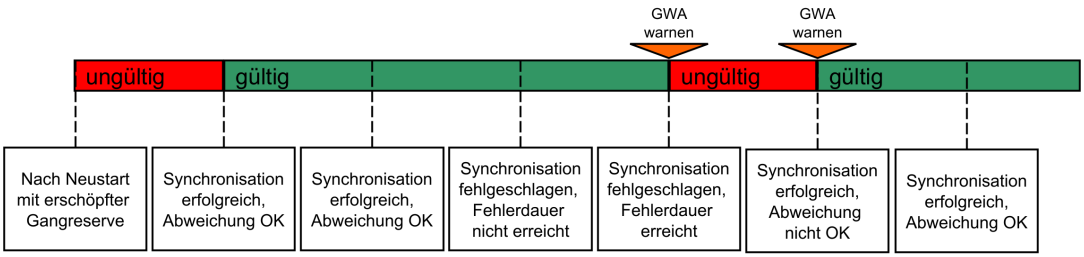


Abbildung 3.17. Status der Systemzeit bei verschiedenen Ereignissen

3.10.5.2 Auslöser

REQ.FA.SyncTimeWithGwa.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Nach dem Neustart des SMGW (▸ICS.WAF2.Zeitsynchronisation.20).
- Periodisch innerhalb der Zeit (▸ICS.FA.TimeSyncWithGwa.90) +/- 1h
- Nach dem Auslösen des Selbsttests (▸FA.DoSelftest) durch GWA oder SRV (▸ICS.WAF2.Zeitsynchronisation.30).

- (▸ICS.WAF2.Zeitsynchronisation.50) Durch den GWA über ▸WKS.MANAGEMENT.

▸ [PTB.13003.1]

3.10.5.3 Anforderungen

- Damit der GWA dauerhafte Störungen der Zeitsynchronisation eines SMGW rechtzeitig erkennt, **MUSS** das SMGW bei erstmaliger Überschreitung der Dauer der ausbleibenden erfolgreichen Zeitsynchronisation (▸ICS.FA.TimeSyncWithGwa.70) den GWA warnen, sofern dieses Datenfeld ungleich 0 ist. ▸ [PTB.13004.1] [REQ.WAN.Zeitsynchronisation.100]
- Sofern die "Zeitsynchronisationsfehlerdauer" (▸ICS.FA.TimeSyncWithGwa.60) überschritten wird, **MUSS** das SMGW den Zeitsynchronisationsstatus ▸timeValid gleich "false" und im kombinierten Statuswort ▸smgwStatus.timeNotValid gleich "true" setzen. ▸ [PTB.13004.2] [REQ.WAF2.Zeitsynchronisation.54] Weitere Maßnahmen, wie z.B. Markierung von Messwerten, sind in den jeweiligen FA-Anforderungen beschrieben.

Durchführung der Zeitsynchronisation

- Das SMGW **MUSS** die Zeitsynchronisation mit dem GWA über das Kommunikationsszenario "WKS.NTP-TLS" durchführen. [REQ.WAN.Kommunikationsszenarien.90]
- Um Delay-Angriffe und Zeitmessungen mit zu langer RTT zu verwerfen, **MUSS** das SMGW empfangene Zeitsynchronisations-Nachrichten mit "rtt" > "maximale Zeitabweichung" (▸ICS.FA.TimeSyncWithGwa.80) verwerfen. ▸ [BSI.13008.1] [REQ.WAN.Zeitsynchronisation.80]
- Das SMGW **MUSS** nach jeder erfolgreichen Synchronisation ▸timeValid in ▸Zeitsynchronisationsstatus gleich "true" und im kombinierten Statuswort ▸smgwStatus.timeNotValid gleich "false" setzen. [REQ.WAF2.Zeitsynchronisation.50]
- Sofern nach einer erfolgreichen Synchronisation die bei der Synchronisation ermittelte Zeitabweichung zur Systemzeit ("deviation") > "maximale Zeitabweichung" (▸ICS.FA.TimeSyncWithGwa.80) - 0,5 * "rtt" beträgt, **MUSS** das SMGW dieses Ereignis protokollieren. ▸ [PTB.13005.1] [REQ.WAF2.Zeitsynchronisation.55]
- Das SMGW **SOLL** mindestens bis zum 31.12.2049 23:59:59 UTC die vom Zeitserver empfangene Zeit korrekt in die Systemzeit umwandeln können. [REQ.WAN.Zeitsynchronisation.110] Der Zeitpunkt wurde so gewählt, dass die Zertifikatsstruktur bis Ende 2049 (siehe RFC5280 Kapitel 4.1.2.5) als auch die Besonderheiten des NTP-Protokolls im Jahr 2036 und 2038 darin eingeschlossen sind.
- Sofern die Synchronisation (unabhängig von der Zeitabweichung) erfolgreich war, **MUSS** das SMGW die Systemzeit gemäß der per Zeitsynchronisation erhaltenen Zeit stellen. ▸ [PTB.13002.0] ▸ [PTB.13002.1] ▸ [PTB.13003.0] . Der GWA wird benachrichtigt, wenn er zuvor gemäß ▸REQ.WAN.Zeitsynchronisation.100 gewarnt wurde. [REQ.WAF2.Zeitsynchronisation.53]
- Das SMGW **MUSS** nach einer erfolgreichen Zeitsynchronisation die Datenfelder ▸currentTime, ▸rtt, ▸deviation, ▸lastDeviationOk, ▸lastSyncTime im ▸Zeitsynchronisationsstatus aktualisieren. [REQ.WAF2.Zeitsynchronisation.51]
- Unmittelbar nach der ersten erfolgreichen Zeitsynchronisation nach Inbetriebnahme **MUSS** das SMGW den Messbetrieb aufnehmen ▸ [FNN.19006.0] [REQ.WAF2.Zeitsynchronisation.60]
- Das SMGW **MUSS** die lokale Zeitzone als Offset zur UTC gemäß [SoZV] zur Ausgabe an den Schnittstellen des SMGW bestimmen. [REQ.FA.SyncTimeWithGwa.20]

Gangreserve bei Ausfall der externen Spannungsversorgung des SMGW

- Die Gangreserve der Systemuhr des SMGW **KANN** über einen Hardware-Baustein (Real-Time-Clock, RTC) realisiert werden, z.B. mit Kondensator/Batteriepufferung im Falle des Ausfalles der Spannungsversorgung des SMGW (Bedingung: ▸ICS.WAF2.Zeitsynchronisation.10). [REQ.WAF2.Zeitsynchronisation.20]
- Falls die Systemuhr des SMGW eine Gangreserve besitzt, **MUSS** das SMGW bei Wiederaufnahme des normalen Betriebs prüfen, ob die Dauer des Ausfalles der Versorgungsspannung der Systemuhr größer war als die "Gangreservedauer" (▸ICS.WAF2.Zeitsynchronisation.10). ▸ [PTB.13001.2] [REQ.WAF2.Zeitsynchronisation.30]

ICS



ICS.WAF2.Zeitsynchronisation.10

Der GWH **MUSS** im ICS die garantierte Gangreservezeit (in Minuten) deklarieren. Besitzt das SMGW keine Gangreserve, ist 0 anzugeben.



ICS.WAF2.Zeitsynchronisation.20

Der GWH **MUSS** im ICS die maximale Zeit bis zum Beginn des Verbindungsaufbaues zur Zeitsynchronisation nach dem Auslösen eines Neustart des SMGW angeben (in Minuten, maximal 10).



ICS.WAF2.Zeitsynchronisation.30

Der GWH **MUSS** im ICS die maximale Zeit bis zum Beginn des Verbindungsaufbaues zur Zeitsynchronisation nach Auslösen des Selbsttests des SMGW angeben (in Minuten, maximal 10).



ICS.WAF2.Zeitsynchronisation.40

Der GWH **MUSS** im ICS deklarieren bis zu welchem Jahr (Mindestens 2032) das SMGW die vom Zeitserver empfangene Zeit korrekt in die Systemzeit umwandeln kann.



ICS.WAF2.Zeitsynchronisation.50

Der GWH **MUSS** im ICS deklarieren, ob der FA durch den GWA ausgelöst werden kann.



ICS.FA.TimeSyncWithGwa.60

Der GWH **MUSS** im ICS deklarieren, nach welcher Zeit (in Sekunden) das SMGW mit ausbleibender erfolgreicher Zeitsynchronisation eine Überschreitung von ZA_{max} annimmt (Zeitsynchronisationsfehlerdauer).



ICS.FA.TimeSyncWithGwa.70

Der GWH **MUSS** im ICS deklarieren, nach welcher Zeit (in Sekunden) das SMGW den GWA bei ausbleibender erfolgreicher Zeitsynchronisation informiert (Zeitsynchronisationswarnzeit).



ICS.FA.TimeSyncWithGwa.80

Der GWH **MUSS** im ICS deklarieren, welche Zeit (in Sekunden) das SMGW als Obergrenze für die zulässige Zeitabweichung verwendet (maximale Zeitabweichung). Hierbei ist zu beachten, dass dieser Wert <= 3 % der kürzesten vom SMGW unterstützten Registrierperiode sein muss.



ICS.FA.TimeSyncWithGwa.90

Der GWH **MUSS** im ICS deklarieren, in welcher Periode (in Stunden) das SMGW regelmäßig die Zeitsynchronisation mit dem GWA durchführt, so dass eine Zeitabweichung von <= 3 % zur gesetzlichen Zeit für die kleinste konfigurierbare Registrierperiode eingehalten werden kann.

Der Wert darf nicht kleiner als 6 Stunden und nicht größer als 7 Tage sein.

Der GWH bemisst die Periode nach der kleinsten und größten berechneten Drift der nicht synchronisierten Systemzeit für die zulässigen Betriebsbedingungen (Temperatur, Feuchte), Bauteilalterungen und Fertigungstoleranzen und stellt die Berechnung in einer Begleitdokumentation für die Prüfstellen bereit.

3.10.5.4 Implementierungshinweise

Um die Stetigkeit und Genauigkeit der Zeitführung zu gewährleisten, soll das SMGW die Zeitführung gemäß [RFC5905] Kapitel 9.2, 10, 11.2, 11.3, 13.2 implementieren.

Die Gangreserve sollte vom Hersteller höchstens so lang gewählt werden, dass unter Berücksichtigung der Langzeitstabilität des Uhrenbausteins (RTC) bei Alterung und Umgebungsbedingungen die hochgerechnete

Abweichung bei Ablauf der Gangreserve gerade die Fehlergrenze (siehe ▸REQ.WAF2.Zeitsynchronisation.50) erreicht hat.

3.10.6 FA.ReadTimeSyncStatus

3.10.6.1 Beschreibung

Das SMGW exportiert die bei der letzten Zeitsynchronisation mit dem Zeitserver ermittelten Statusinformationen des Zeitsynchronisationsprotokolls (TimeSyncStatus) und die aktuelle Zeit mit Bezug zur lokalen Zeit.

Die Systemzeit des SMGW wird regelmäßig mit dem GWA-Zeitserver synchronisiert, der mit der gesetzlichen Zeit synchronisiert ist. Die an den Aufrufer exportierten Informationen ermöglichen ihm eine Prüfung der Zeitführung des SMGW und den Bezug der Systemzeit in einem Format gemäß [RFC3339].

Der Aufrufparameter identifiziert das Gerät, dessen Systemzeit abgefragt wird. Ist die SMGW-ID angegeben bezieht sich die Abfrage auf das SMGW, ist eine Zähler-ID angegeben bezieht sich die Abfrage auf den Zähler (siehe ▸FA.RetrieveClockStateFromMtr).

3.10.6.2 Auslöser



REQ.FA.ReadTimeSyncStatus.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Empfang einer Anfrage über ▸HKS.WS1.
- Empfang einer Anfrage über ▸HKS.WS2.

3.10.6.3 Anforderungen

- (Geräte-ID im Aufrufparameter entspricht der SMGW-ID) Das SMGW **MUSS** den Status der Systemuhr gemäß ▸Zeitsynchronisationsstatus an den Aufrufer übermitteln. Ist die ▸timeValid gleich "false", entfällt das Datenfeld ▸currentTime. Solange keine Zeitsynchronisation durchgeführt wurde, entfällt das Datenfeld ▸lastSyncTime. [REQ.FA.ReadTimeSyncStatus.20]
- (Geräte-ID im Aufrufparameter entspricht einer ▸meterId eines LMN-Kommunikationsprofils für LKS1) Das SMGW **MUSS+** den Status der Zeitsynchronisation aus der Messeinrichtung über ▸FA.RetrieveClockStateFromMtr abfragen und das Ergebnis an den Aufrufer übermitteln. [REQ.FA.ReadTimeSyncStatus.30]

3.10.7 FA.NtpTimeService

3.10.7.1 Beschreibung

Das SMGW stellt die (mit der gesetzlichen Zeit synchronisierte) Systemzeit zur Zeitsynchronisation automatisiert arbeitenden Geräte bereit.

In der Antwort liefert das SMGW die Systemzeit, den Zeitsynchronisationsstatus, die Abweichung der Systemzeit vom Root-Zeitserver und Informationen über Laufzeit und Genauigkeit.

Informationen über die lokale Zeitzone bzw. der Offset der lokalen Zeitzone zur UTC werden nicht übermittelt.

Das SMGW unterstützt die NTP-Betriebsart "server".

3.10.7.2 Auslöser



REQ.FA.NtpTimeService.20

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anforderung über ▸HKS.NTP-TLS.SRV.

3.10.7.3 Anforderungen

- Das SMGW **MUSS** die Systemzeit des SMGW für die NTP-Era gleich 0 an den Aufrufer übermitteln können (bis 8. Februar 2036). [REQ.FA.NtpTimeService.30]

- Das SMGW **SOLL** die Systemzeit des SMGW für die NTP-Era gleich 1 an den Aufrufer übermitteln können (ab 8. Februar 2036). [REQ.FA.NtpTimeService.40]
- Das SMGW **MUSS** mindestens eine Granularität (Präzision) der exportieren Systemzeit von einer Sekunde unterstützen. [REQ.FA.NtpTimeService.50]
- Das SMGW **MUSS** dem Aufrufer den Fehler der Systemzeit vom Root-Zeitserver übermitteln (Root Delay, Root Dispersion). [REQ.FA.NtpTimeService.60]
- Das SMGW **MUSS** eine NTP-Anfrage in 90% der Anfragen innerhalb von einer Sekunde beantworten. [REQ.FA.NtpTimeService.70]
- Um eine Überlastung des SMGW zu vermeiden **MUSS** das SMGW die NTP-Anfrage von nicht authentifizierten Clients nach 5 Anfragen innerhalb einer Minute für eine Stunde nicht mehr beantworten. [REQ.FA.NtpTimeService.80]

ICS



ICS.FA.NtpTimeService.10

Der GWH **MUSS** im ICS deklarieren, ob das SMGW im NTP-Zeitserver die Systemzeit mit der NTP-Era "1" übermitteln kann.

3.11 Anbindung von Messeinrichtungen im LMN administrieren (FAKAT.LmnComConfig)

3.11.1 Übersicht

Die Anwendungsfälle dieser Kategorie unterstützen den GWA bei der Konfiguration der kommunikativen Anbindung von Messeinrichtungen an das SMGW.

Anwendungsfälle zur Kommunikation mit Messeinrichtungen nach erfolgter kommunikativer Anbindung finden sich in ▸FAKAT.MtrServices und ▸FAKAT.ValCapture.

3.11.2 Übersicht der FA

Aufgabe	Umsetzung
Kommunikationsparameter zur kommunikativen Anbindung einer Messeinrichtung durch GWA importieren	Das SMGW **MUSS** ▸FA.CreateLmnComProfile für den GWA umsetzen. [REQ.WAN.Management.10]
Kommunikationsparameter zur kommunikativen Anbindung einer Messeinrichtung durch GWA aktualisieren	Das SMGW **MUSS** ▸FA.UpdateLmnComProfile für den GWA umsetzen. [REQ.WAN.Management.11]
kommunikative Anbindung einer Messeinrichtung durch GWA entfernen	Das SMGW **MUSS** ▸FA.DeleteLmnComProfile für den GWA umsetzen. [REQ.WAN.Management.20]
Konfiguration der kommunikativen Anbindung einer Messeinrichtung durch GWA auslesen	Das SMGW **MUSS** ▸FA.ReadLmnComProfile für den GWA umsetzen. [REQ.FAKAT.LmnComConfig.20]
Kommunikativ angebundene und anbindbare Messeinrichtungen durch GWA abfragen	Das SMGW **SOLL** ▸FA.ListIdentifiedMeters für den GWA umsetzen. [REQ.WAN.Management.30]
Pairing von SMGW und bidirektional kommunizierender Messeinrichtung	Das SMGW **MUSS** ▸FA.DoInitialMtrSmgwPairing für den GWA umsetzen. [REQ.LMN.Zaehlerverwaltung.20]
Zertifikatserneuerung der Messeinrichtung	Das SMGW **MUSS** ▸FA.DoRenewMtrCertificate für den GWA umsetzen. [REQ.LMN.Zaehlerverwaltung.30]
(Neues) Zertifikat zur Authentifizierung des SMGW als Vertrauensanker an die Messeinrichtung übermitteln	Das SMGW **MUSS** ▸FA.DoExportSmgwLmnCertToMtr für den GWA umsetzen. [REQ.LMN.Zaehlerverwaltung.40]

Aufgabe	Umsetzung
Erzeugen eines neuen SMGW-LMN-Schlüsselpaares und selbstsignierten Zertifikates ausgelöst durch den GWA	Siehe ▸FA.DoCreateSelfsignedSmgwLmnCert
Nicht benötigtes Schlüsselpaar und selbstsigniertes TLS-Zertifikat des SMGW im LMN durch GWA deaktivieren	Siehe ▸FA.DoDeactivateSelfsignedSmgwLmnCert.
Test der kommunikative Anbindung eines Zählers durch GWA auslösen	Das SMGW **SOLL** auf Anforderung und regelmäßig selbstständig die Zuverlässigkeit der LMN-Kommunikation prüfen. [REQ.WAN.Selbsttest.40]

Tabelle 3.30 Übersicht der FA der Kategorie FAKAT.LmnComConfig

ICS



ICS.WAN.Selbsttest.30

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



ICS.FAKAT.LmnComConfig.10

Der GWH **MUSS** im ICS angeben, ob das SMGW ▸Abschnitt 3.11.11 für die Rolle GWA anbietet.

3.11.3 Datenstrukturen

Das LMN-Kommunikationsprofil ist in ▸Abschnitt 3.22.25 beschrieben.

Die Datenstruktur Zählerstatusliste ist in ▸Abschnitt 3.22.29 beschrieben.

3.11.4 FA.CreateLmnComProfile

3.11.4.1 Beschreibung

Nach erfolgreicher Prüfung des Aufrufparameters des LMN-Kommunikationsprofiles gemäß ▸LMN-Kommunikationsprofil (Zählerprofil) persistiert das SMGW das Kommunikationsprofil für eine neu kommunikativ anzubindende Messeinrichtung. Die Konfigurationsparameter identifizieren die Messeinrichtung und dienen der Vorbereitung der authentischen initialen kommunikativen Anbindung.

3.11.4.2 Auslöser



REQ.FA.CreateLmnComProfile.80

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.11.4.3 Anforderungen

- Das SMGW **MUSS** LMN-Kommunikationsprofile mit identischem Datenfeld ▸meterId, bereits beim Konfigurieren der LMN-Kommunikationsprofil im SMGW ablehnen. ▸ [FNN.20005.4] [REQ.FA.CreateLmnComProfile.40]
- Das SMGW **SOLL** die Datenfelder gemäß ▸Tabelle 3.31 auf Plausibilität prüfen und im Fehlerfall den Import ablehnen. ▸ [FNN.20005.3] [REQ.FA.CreateLmnComProfile.41]
- Das SMGW **MUSS** das LMN-Kommunikationsprofil persistieren und den oder die darin enthaltenen Kommunikationsschlüssel für die Authentifizierung der Kommunikation mit der darin identifizierten Messeinrichtung verwenden. ▸ [BSI.20005.0] [REQ.FA.CreateLmnComProfile.50] [11]

[11] Bei LKS2 wird der Kommunikationsschlüssel für die Authentifizierung und Entschlüsselung empfangener Nachrichten verwendet, bei LKS1 für die initiale kommunikative Anbindung über das symmetrische Verfahren mittels ▸LKS1.PSK.

Nr.	Bedingung	Datenfeld	Prüfung
1	▸ks gleich "LKS1"	▸mtrTlsCert, ▸pairingKey	Eines von beiden muss für die initiale kommunikative Anbindung vorhanden sein. ▸pairingKey wird für ▸LKS1.PSK benötigt.
2	▸ks gleich "LKS2"	▸pairingKey	Ist vorhanden.
3	Immer	▸smgwTlsCert	Ist nicht vorhanden.
4	Immer	▸mtrTlsCert	Sofern das initiale Pairing-Zertifikat vorhanden ist muss es den Vorgaben gemäß [DS] "Zertifikate im LMN" für Messeinrichtungen entsprechen.

Tabelle 3.31 Plausibilitätsprüfungen

ICS



ICS.FA.CreateLmnComProfile.10

Der GWH **MUSS** im ICS deklarieren, wie viele LKS1-Messeinrichtungen das SMGW kommunikativ anbinden kann.



ICS.FA.CreateLmnComProfile.20

Der GWH **MUSS** im ICS deklarieren, wie viele LKS2-Messeinrichtungen das SMGW kommunikativ anbinden kann.



ICS.FA.CreateLmnComProfile.30

Der GWH **MUSS** im ICS deklarieren, welche Plausibilitätsprüfungen gemäß ▸Tabelle 3.31 das SMGW durchführt.

3.11.5 FA.UpdateLmnComProfile

3.11.5.1 Beschreibung

Das SMGW erwartet als Aufrufparameter ein LMN-Kommunikationsprofil gemäß ▸LMN-Kommunikationsprofil (Zählerprofil) für eine bereits kommunikativ angebundene Messeinrichtung. Das LMN-Kommunikationsprofil wird aktualisiert und persistiert.

3.11.5.2 Auslöser



REQ.FA.UpdateLmnComProfile.60

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.11.5.3 Anforderungen

- Das SMGW **SOLL** die Datenfelder gemäß ▸Tabelle 3.31 auf Plausibilität prüfen und im Fehlerfall den Import ablehnen. ▸ [FNN.20006.3] [REQ.FA.UpdateLmnComProfile.15]
- Das SMGW **MUSS** den Import ablehnen, sofern durch den Aufrufparameter Datenfelder gemäß ▸Tabelle 3.32 geändert würden. ▸ [FNN.20006.4] [REQ.FA.UpdateLmnComProfile.16]
- Das SMGW **MUSS** für fehlende optionale Datenfelder im Aufrufparameter die entsprechenden bereits konfigurierten Daten unverändert lassen. [REQ.FA.UpdateLmnComProfile.10]
- Das SMGW **MUSS** die Änderungen persistieren und künftig für die Kommunikation mit der Messeinrichtung verwenden. ▸ [BSI.20006.0] [REQ.FA.UpdateLmnComProfile.30]

Nr.	Bedingung	Datenfeld	Prüfung
1	Immer	▸ks	Unverändert gegenüber dem im SMGW konfigurierten ▸ks

Nr.	Bedingung	Datenfeld	Prüfung
2	Immer	▸meterId	Unverändert gegenüber der SMGW konfigurierten ▸meterId

Tabelle 3.32 Plausibilitätsprüfungen

3.11.6 FA.DeleteLmnComProfile

3.11.6.1 Beschreibung

Das SMGW entfernt das über den Aufrufparameter identifizierte LMN-Kommunikationsprofil und die Kommunikative Anbindung im SMGW, so dass die kommunikative Anbindung der Messeinrichtung an das SMGW aufgehoben ist.

3.11.6.2 Auslöser



REQ.FA.DeleteLmnComProfile.30

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.11.6.3 Anforderungen

- Das SMGW **MUSS** die Löschung des LMN-Kommunikationsprofils ablehnen, wenn das Profil aufgrund der Vorhaltefrist zur Einhaltung der referenziellen Integrität von ▸meterId gemäß ▸Abschnitt 5.5 nicht gelöscht werden darf. [REQ.FA.DeleteLmnComProfile.10]
- Sofern ein Firmware-Updateprofil mit der Geräte-ID ▸meterId im zu löschenden LMN-Kommunikationsprofil verknüpft ist, **MUSS** das SMGW ▸FA.DeleteFwUpdateConfig aufrufen. [REQ.FA.DeleteLmnComProfile.11]
- Das SMGW **MUSS** das LMN-Kommunikationsprofil so löschen, dass es nicht mehr für die Kommunikation der darin identifizierten Messeinrichtung mit dem SMGW verwendet werden kann. ▸ [FNN.20009.0] [REQ.FA.DeleteLmnComProfile.20]

3.11.7 FA.ReadLmnComProfile

3.11.7.1 Beschreibung

Das SMGW exportiert auf Anforderung das im Aufrufparameter identifizierte LMN-Kommunikationsprofil.

Das LMN-Kommunikationsprofil enthält die aktuellen Konfigurationsparameter zur Kommunikation zwischen SMGW und Messeinrichtung, wie z.B. das zur bidirektionalen Kommunikation mit der Messeinrichtung verwendete MTR_LMN_TLS_CRT- und GW_LMN_TLS_CRT-Zertifikat.

Das ausgelesene LMN-Kommunikationsprofil enthält keine geheimen Schlüssel.

3.11.7.2 Auslöser



REQ.FA.ReadLmnComProfile.20

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle SRV.

3.11.7.3 Anforderungen

Das SMGW **MUSS** das im Aufrufparameter identifizierte, persistierte LMN-Kommunikationsprofil gemäß ▸LMN-Kommunikationsprofil (Zählerprofil) ohne das Datenfeld ▸pairingKey exportieren. ▸ [BSI.20030.0] [REQ.FA.ReadLmnComProfile.10]

3.11.8 FA.DoInitialMtrSmgwPairing

3.11.8.1 Beschreibung

Das SMGW erzeugt für die bidirektional kommunizierende Messeinrichtung unter Berücksichtigung der [TR-03109-3] und den Vorgaben der Aufrufparameters (▸namedCurveId) ein neues Schlüsselpaar und ein damit signiertes TLS-Zertifikat gemäß [DS] Kapitel "LMN-Zertifikatsprofile".

Das SMGW exportiert den privaten Schlüssel MTR_LMN_TLS_PRV, das zugehörige Zertifikat MTR_LMN_TLS_CRT und das aktuelle LMN-TLS-Zertifikat des SMGW (GW_LMN_TLS_CRT) vertraulich und authentisch an die authentifizierte und identifizierte Messeinrichtung.

Die initiale authentische Übermittlung kann entweder über einen zuvor vom Zählerhersteller zum GWA vertraulich und authentisch übermittelten geräteindividuellen, gemeinsamen geheimen Schlüssel (Kommunikationsszenario LKS1.PSK) oder über ein zuvor vom Zählerhersteller zum GWA authentisch übermitteltes initiales Zählerzertifikat (MTR_LMN_TLS_CRT_0) erreicht werden.

Die Messeinrichtung verwendet das vom SMGW erzeugte neue MTR_LMN_TLS_CRT_1-Zertifikat künftig für die Absicherung der Kommunikation mit dem SMGW.

3.11.8.2 Auslöser



REQ.FA.DoInitialMtrSmgwPairing.70

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Das LMN-Kommunikationsprofil für LKS1 wurde konfiguriert (▸FA.CreateLmnComProfile).

3.11.8.3 Anforderungen

- (Aufruf via ▸WKS.MANAGEMENT) Das SMGW **MUSS** den Aufruf ablehnen, wenn zu der im Aufrufparameter identifizierten Messeinrichtung kein LMN-Kommunikationsprofil im SMGW aktiv ist. [REQ.FA.DoInitialMtrSmgwPairing.10]
- (Aufruf via ▸WKS.MANAGEMENT) Das SMGW **MUSS** den Aufruf ablehnen, wenn das der Messeinrichtung zugeordnete LMN-Kommunikationsprofil nicht vom Typ ▸ks gleich "LKS1" ist. [REQ.FA.DoInitialMtrSmgwPairing.50]
- Das SMGW **MUSS** das Schlüsselpaar MTR_LMN_TLS_PRV/PUB und das TLS-Zertifikat MTR_LMN_TLS_CRT für die Messeinrichtung gemäß Aufrufparameter (▸Parametersatz für Schlüssel- und Zertifikats-Erzeugung) erzeugen. ▸ [BSI.1017.1] [REQ.FA.DoInitialMtrSmgwPairing.20]
- Sofern im Kommunikationsprofil ein PSK (▸pairingKey) konfiguriert ist, **MUSS** das SMGW das initiale Pairing gemäß [DS] Kapitel "Bidirektionale LMN-Kommunikation über HDLC" über ▸LKS1.PSK vertraulich und authentisch ausführen, um das Zählerzertifikat MTR_LMN_TLS_CRT, den zugehörigen privaten Schlüssel MTR_LMN_TLS_PRV und das SMGW-Zertifikat GW_LMN_TLS_CRT an die Messeinrichtung zu übermitteln. ▸ [BSI.1017.2] ▸ [BSI.1017.0] [REQ.FA.DoInitialMtrSmgwPairing.30]
- Sofern im Kommunikationsprofil kein PSK (▸pairingKey), dafür aber ein Zählerkommunikationszertifikat (▸mtrTlsCert) konfiguriert ist, **MUSS+** das SMGW das künftige MTR_LMN_TLS_CRT_1, den zugehörigen privaten Schlüssel MTR_LMN_TLS_PRV und das SMGW-Zertifikat GW_LMN_TLS_CRT gemäß Detailspezifikation "Bidirektionale LMN-Kommunikation über HDLC" über die mit MTR_LMN_TLS_CRT_0 authentifizierte ▸LKS1 Verbindung vertraulich und authentisch übermitteln. ▸ [BSI.1017.2] ▸ [BSI.1017.0] [REQ.FA.DoInitialMtrSmgwPairing.40]
- Nach erfolgreicher Übermittlung von MTR_LMN_TLS_CRT, GW_LMN_TLS_CRT an die Messeinrichtung **MUSS** das SMGW das Datenfeld ▸mtrTlsCert im LMN-Kommunikationsprofil der Messeinrichtung gleich MTR_LMN_TLS_CRT_1 und das Datenfeld ▸smgwTlsCert gleich GW_LMN_TLS_CRT setzen. [REQ.FA.DoInitialMtrSmgwPairing.60]

ICS



ICS.FA.DoInitialMtrSmgwPairing.10

Der GWH **MUSS** im ICS deklarieren, ob das SMGW das Pairing ohne PSK mit einem Initialen Zählerzertifikat MTR_LMN_TLS_CRT$_0$ unterstützt.

3.11.8.4 Implementierungshinweise

Das EC-Schlüsselpaar gemäß [TR-03111] wird mit dem Zufallszahlengenerator (des Sicherheitsmodules) erzeugt. Da das Schlüsselpaar an die Messeinrichtung exportiert wird, wird das Schlüsselpaarobjekt nicht im Sicherheitsmodul erzeugt.

Da das Schlüsselpaar nach Erzeugung des selbstsignierten TLS-Zertifikates der Messeinrichtung und nach der Übermittlung an die Messeinrichtung nicht mehr vom SMGW benötigt wird, soll es nach dem Pairing zwischen SMGW und Messeinrichtung gelöscht werden.

3.11.9 FA.DoExportSmgwLmnCertToMtr

3.11.9.1 Beschreibung

Das SMGW exportiert das künftige GW_LMN_TLS_CRT$_{n+1}$ an die Messeinrichtung, damit diese das Zertifikat künftig für die SMGW-Authentifizierung verwendet.

Die Aktualisierung wird vor Ende der Laufzeit gemäß [TR-03109-3] durch den GWA initiiert.

Sofern ein Aufrufparameter eine Messeinrichtung identifiziert, bezieht sich der FA auf diese Messeinrichtung.

3.11.9.2 Auslöser



REQ.FA.DoExportSmgwLmnCertToMtr.20

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Ein Schlüsselpaar und GW_LMN_TLS_CRT des SMGW wurde erzeugt (▸FA.DoCreateSelfsignedSmgwLmnCert).

3.11.9.3 Anforderungen

- Das SMGW **MUSS** das künftige GW_LMN_TLS_CRT$_{n+1}$ gemäß Detailspezifikation "Bidirektionale LMN-Kommunikation über HDLC" über das ▸LKS1 an die Messeinrichtung übertragen und bei erfolgreicher Aktualisierung im Datenfeld ▸smgwTlsCert im LMN-Kommunikationsprofil persistieren. ▸[FNN.17016.0] ▸[FNN.17016.1] [REQ.FA.DoExportSmgwLmnCertToMtr.10]
- Sofern der Aufruf durch das SMGW automatisiert nach Erzeugen von GW_LMN_TLS_CRT aufgerufen wird, **MUSS** das SMGW ▸REQ.FA.DoExportSmgwLmnCertToMtr.10 für jede kommunikativ angebundenen Messeinrichtung durchführen. [REQ.FA.DoExportSmgwLmnCertToMtr.30]

3.11.10 FA.DoRenewMtrCertificate

3.11.10.1 Beschreibung

Das SMGW erstellt gemäß Aufrufparameter (▸namedCurveId) ein neues Schlüsselpaar und Zertifikat für die Messeinrichtung und exportiert das künftige MTR_LMN_TLS_CRT$_{n+1}$ und den privaten Schlüssel MTR_LMN_TLS_PRV$_{n+1}$ an die Messeinrichtung, damit diese das Zertifikat künftig für die TLS-Kommunikation verwendet.

3.11.10.2 Auslöser



REQ.FA.DoRenewMtrCertificate.20

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

- Automatisiert durch das SMGW vor Ablauf des MTR_LMN_TLS_CRT (▸ICS.FA.DoRenewMtrCertificate.10).

3.11.10.3 Anforderungen

- Das SMGW **MUSS** LMN-Zertifikate nach Detailspezifikation [DS] "Zertifikate im LMN" unter Berücksichtigung des Aufrufparameters (▸namedCurveId) für die Zähler erstellen. ▸ [BSI.1017.1] [REQ.LMN.TlsSicherung.70]
- Das SMGW **MUSS** das künftige MTR_LMN_TLS_CRT$_{n+1}$ gemäß Detailspezifikation "Bidirektionale LMN-Kommunikation über HDLC" über das ▸LKS1 an die Messeinrichtung übertragen und bei erfolgreicher Aktualisierung im Datenfeld ▸mtrTlsCert des LMN-Kommunikationsprofiles persistieren. ▸ [BSI.1017.2] ▸ [BSI.1017.0] [REQ.FA.DoRenewMtrCertificate.10]

ICS



ICS.FA.DoRenewMtrCertificate.10

Der GWH **MUSS** im ICS deklarieren, wie lange vor Ablauf des MTR_LMN_TLS-Zertifikates (Datenfeld valid.notAfter) das SMGW automatisiert die Erneuerung des Zählerzertifikates auslöst (Angabe in Tagen). Wird ein Wert 0 angegeben, wird das Zählerzertifikat nicht automatisiert durch das SMGW erneuert.

3.11.10.4 Implementierungshinweise

Das EC-Schlüsselpaar gemäß [TR-03111] wird mit dem Zufallszahlengenerator (des Sicherheitsmodules) erzeugt. Da das Schlüsselpaar an die Messeinrichtung exportiert wird, wird das Schlüsselpaarobjekt nicht im Sicherheitsmodul erzeugt.

Da das Schlüsselpaar nach Erzeugung des selbstsignierten TLS-Zertifikates der Messeinrichtung und nach der Übermittlung an die Messeinrichtung nicht mehr vom SMGW benötigt wird, soll es nach dem Pairing zwischen SMGW und Messeinrichtung gelöscht werden.

3.11.11 FA.ListIdentifiedMeters

3.11.11.1 Beschreibung

Das SMGW exportiert die Liste der Geräte-IDs der im LMN (drahtlos und leitungsgebunden) kommunikativ erreichbaren Messeinrichtungen und den Status ihrer kommunikativen Anbindung.

Dieser FA unterstützt GWA und Servicetechniker bei der Diagnose zur kommunikativen Anbindung von Messeinrichtungen an das SMGW.

Folgende Zustände werden bei der Auflistung der kommunikativ erreichbaren Messeinrichtungen unterschieden:

- PROFILE_ONLY: kennzeichnet den Zustand, wenn ein LMN-Kommunikationsprofil konfiguriert ist, ohne dass die Messeinrichtung im Netzwerk identifiziert wurde.
- IDENTIFIED: kennzeichnet den Zustand, wenn eine Messeinrichtung über eine Kommunikationsadresse erreichbar ist und noch kein Pairing über den Kommunikationsschüssel erfolgt ist. Da der Zähler nicht authentifiziert ist, kann die Lebensdauer dieser Listeneinträge begrenzt werden.
- AUTHENTICATED: kennzeichnet den Zustand, wenn das Pairing mit dem Kommunikationsschlüssel (PSK oder initiales Gerätezertifikat) erfolgt ist, aber noch keine Messwertnachricht entschlüsselt wurde.
- DATA_EXCHANGE: kennzeichnet den Zustand, wenn mindestens eine empfangene Nachricht erfolgreich entschlüsselt wurde.

Die Semantik der bereitgestellten Informationen ist abhängig vom Kommunikationsszenario wie folgt:

- Für Messeinrichtungen, die über LKS1 bedrahtet kommunizieren, enthält ▸meter.l2Address die in der automatischen Adressvergabe zugeteilte HDLC-Adresse.
- Für Messeinrichtungen, die über LKS2 drahtlos kommunizieren enthält ▸meter.l2Address die für die Funkübertragung genutzte Data-Link-Layer-Adresse.

- Für Messeinrichtungen, die über LKS2 drahtlos kommunizieren kann die Qualität des Funkempfangs (Empfangsfeldstärke des Signals) geprüft werden (▸meter.rssi).

Die Aufzeichnung des letzten Empfangszeitpunktes einer Nachricht ermöglicht die zeitliche Zuordnung zu physischen Ereignissen, die zu Übertragungsstörungen führen.

3.11.11.2 Auslöser



REQ.FA.ListIdentifiedMeters.50

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle SRV.

3.11.11.3 Anforderungen

- Das SMGW **MUSS** die im SMGW identifizierten und sichtbaren Messeinrichtungen für den Aufrufer mithilfe der ▸Zählerstatusliste auflisten. [REQ.FA.ListIdentifiedMeters.10]
- Das SMGW **MUSS** das Datenfeld ▸meter.ks gemäß konfiguriertem LMN-Kommunikationsprofil ▸ks setzen. Ist für die Messeinrichtung kein LMN-Kommunikationsprofil konfiguriert entfällt das Datenfeld. [REQ.FA.ListIdentifiedMeters.20]
- Das SMGW **MUSS** das Datenfeld ▸meter.lastTs auf den Zeitpunkt des letzten Empfangs einer Messwertnachricht von der Messeinrichtung setzen. [REQ.FA.ListIdentifiedMeters.30]
- Das SMGW **MUSS** das Datenfeld ▸meter.pairingState gemäß ▸Tabelle 3.33 setzen. [REQ.FA.ListIdentifiedMeters.40]

Datenfeld "pairingState"	Bedeutung
PROFILE_ONLY	Ein LMN-Kommunikationsprofil ist für die Messeinrichtung konfiguriert. Die Messeinrichtung wurde noch nicht im LMN identifiziert. D.h. es wurde noch keine Nachricht (Layer 2/3) von der Messeinrichtung empfangen.
IDENTIFIED	Die Messeinrichtung wurde im LMN identifiziert, d.h. es wurde eine Nachricht (Layer 2/3) von der Messeinrichtung empfangen, allerdings ist noch kein Pairing über den Kommunikationsschüssel erfolgt. Dieser Zustand kann vorliegen, wenn noch kein LMN-Kommunikationsprofil konfiguriert ist.
AUTHENTICATED	Das Pairing mit dem Kommunikationsschlüssel ist erfolgt; es wurde noch keine Messwertnachricht entschlüsselt.
DATA_EXCHANGE	Mindestens eine Messwertnachricht wurde erfolgreich entschlüsselt.

Tabelle 3.33 Bedeutung des Pairing-State der Messeinrichtung

ICS



ICS.FA.ListIdentifiedMeters.10

Der GWH **MUSS** im ICS angeben, ob auch Zähler in die Liste als IDENTIFIED aufgenommen werden, für die kein LMN-Kommunikationsprofil konfiguriert ist.



ICS.FA.ListIdentifiedMeters.20

Der GWH **MUSS** im ICS angeben, nach welcher Zeit (in Minuten, aufgerundet) identifizierte, aber nicht authentifizierte Zähler (IDENTIFIED) aus der Liste entfernt werden. Der Wert 0 gibt an, Zähler nicht automatisch aus der Liste entfernt werden.

3.12 Anbindung von EMT administrieren (FAKAT.EmtComConfig)

3.12.1 Übersicht

Dieses Kapitel enthält die fachlichen Anwendungsfälle, die für die kommunikative Anbindung der externen Marktteilnehmer (EMT) an das SMGW benötigt werden. Dies umfasst die Konfiguration zur Herstellung der

Kommunikation zwischen SMGW und EMT, die Erneuerung von Zertifikaten, das Ändern von Kommunikationsparametern und das Auflösen der kommunikativen Anbindung des EMT.

Für die Kommunikation mit dem EMT müssen folgende Kommunikationsparameter im SMGW vorliegen:

- Gültige Zertifikate des EMT aus der SM-PKI für die Inhaltsdatenverschlüsselung, TLS-Authentifizierung und - Anwendungsfallabhängig - zur Signaturvalidierung.
- WAN-Kommunikationsprofile mit Parametern, die das Kommunikationsszenario und den zuverlässigen und sicheren Verbindungsaufbau zum Kommunikationssystem des EMT oder des GWA bestimmen.

Der GWA ist verantwortlich für das Deaktivieren und Entfernen nicht mehr benötigter Zertifikate und WAN-Kommunikationsprofile aus dem SMGW.

3.12.2 Übersicht der FA

Aufgabe	Umsetzung
Kommunikationsparameter und Zertifikate für die kommunikative WAN-Anbindung eines EMT durch GWA importieren	Das SMGW **MUSS** ▸FA.CreateWanComProfile für den GWA umsetzen. [REQ.WAN.Management.140]
Kommunikationsparameter und Zertifikate für die Kommunikative WAN-Anbindung eines EMT durch GWA aktualisieren	Das SMGW **MUSS** ▸FA.UpdateWanComProfile für den GWA umsetzen. [REQ.FAKAT.EmtComConfig.30]
Konfiguration der kommunikativen Anbindung eines EMT durch GWA auslesen	Siehe ▸FA.ReadWanComProfile
Kommunikationsparameter und Zertifikate für die Kommunikative WAN-Anbindung eines EMT durch GWA löschen	Das SMGW **MUSS** ▸FA.DeleteWanComProfile für den GWA umsetzen. [REQ.WAN.Management.150]
Kommunikation mit dem EMT durch den GWA prüfen	Das SMGW **SOLL** ▸FA.DoRequestWanComTest für den GWA umsetzen.(Bedingung: ▸ICS.FAKAT.EmtComConfig.10) [REQ.FAKAT.EmtComConfig.40]

Tabelle 3.34 Übersicht der FA der Kategorie FAKAT.EmtComConfig

ICS



ICS.FAKAT.EmtComConfig.10

Der GWH **MUSS** im ICS beschreiben, ob Kommunikationsselbsttest zum EMT gemäß ▸FA.DoRequestWanComTest implementiert ist.

3.12.3 Datenstrukturen der FA-Kategorie

Die Datenstruktur des EMT-WAN-Kommunikationsprofiles ist in ▸Abschnitt 3.22.46 beschrieben.

3.13 Anbindung von HAN-Teilnehmern administrieren (FAKAT.HanUserConfig)

3.13.1 Übersicht

Bevor lokale Nutzer auf Ressourcen des SMGW zugreifen dürfen, muss der GWA über ▸HAN-Kommunikationsprofil die Informationen zur Rolle, Identifikation und Authentisierung des lokalen Nutzers im SMGW konfigurieren. Lokale Nutzer sind beispielsweise Letztverbraucher bzw. Anschlussnutzer (Rolle *CON*) oder Servicetechniker (Rolle *SRV*) aber auch steuerbare lokale Systeme (Rolle *CLS*). Der Rolle *CON* ist über das HAN-Kommunikationsprofil ein mit dem Auswertungsprofil zugeordnetes Anschlussnutzer-Konto zugeordnet. Die Rolle *SRV* hat keinen Zugriff auf Messwerte, kann den GWA an der Messstelle bei der Diagnose unterstützen, bspw. wenn keine WAN-Kommunikation möglich ist. Der Rolle *CLS* kann optional Zugriff auf eine Teilmenge der Informationen eines Anschlussnutzer-Kontos gewährt werden.

Das SMGW erteilt die Zugriffsberechtigung anhand eines im SMGW konfigurierten HAN-Kommunikationsprofiles. Das SMGW wählt das geeignete HAN-Kommunikationsprofil bei einer ankommenden Verbindungsanforderung über die Übereinstimmung mit den im Verbindungsaufbau präsentierten Adress- und Identifikationsdaten aus und akzeptiert die Verbindungsanfrage nur bei erfolgreicher Authentifizierung mit den Credentials des HAN-Kommunikationsprofiles.

Nachdem ein lokaler Nutzer keine Berechtigung zum Zugriff auf das SMGW mehr benötigt, entfernt der GWA das dem lokalen Nutzer zugeordnete HAN-Kommunikationsprofil.

Der GWA kann die Credentials (Zertifikat, Passwort-Hash) im HAN-Kommunikationsprofil aktualisieren.

3.13.2 Übersicht der FA

Aufgabe	Umsetzung
Konfiguration zur HAN-Kommunikation und Berechtigung eines lokalen Nutzers durch GWA importieren	Das SMGW **MUSS** ▸FA.CreateHanComProfile für den GWA umsetzen. [REQ.WAN.Management.40]
Konfiguration zur HAN-Kommunikation und Berechtigung eines lokalen Nutzers durch GWA aktualisieren	Das SMGW **MUSS** ▸FA.UpdateHanComProfile für den GWA umsetzen. [REQ.WAN.Management.41]
Konfiguration zur HAN-Kommunikation und kommunikativen Anbindung und Berechtigung eines lokalen Nutzers durch GWA löschen	Das SMGW **MUSS** ▸FA.DeleteHanComProfile für den GWA umsetzen. [REQ.WAN.Management.50]
HAN-Kommunikationsprofil an GWA exportieren	Das SMGW **MUSS** ▸FA.ReadHanComProfile für den GWA umsetzen. [REQ.FAKAT.HanUserConfig.20]
CLS im HAN auflisten	Das SMGW **SOLL** ▸FA.ListIdentifiedCls für den GWA umsetzen. (▸ICS.FAKAT.HanUserConfig.10) [REQ.FAKAT.HanUserConfig.30]

Tabelle 3.35 Übersicht der FA der Kategorie FAKAT.HanUserConfig

ICS



ICS.FAKAT.HanUserConfig.10

Der GWH **MUSS** im ICS deklarieren, ob das SMGW den ▸FA.ListIdentifiedCls für den GWA unterstützt.

3.13.3 Datenstrukturen der FA-Kategorie

Das HAN-Kommunikationsprofil ist in ▸Abschnitt 3.22.22 beschrieben.

Die Datenstruktur zur Auflistung der CLS ist in ▸Abschnitt 3.22.12 beschrieben.

3.13.4 FA.CreateHanComProfile

3.13.4.1 Beschreibung

Dieser FA richtet eine Zugriffsberechtigung auf Ressourcen des SMGW für einen lokalen Nutzers im HAN (Rolle CON, SRV, CLS) ein. Das HAN-Kommunikationsprofil verknüpft die Identifikation und Authentifizierung des Nutzers (über "peerCert" oder "userCredentials") mit einer "userId" (Anschlussnutzer-Kennung oder CLS-ID).

Die Zugriffskontrolle auf Messwerte und Anschlussnutzer-Log-Einträge geschieht über ein mit der "profileId" verknüpftes Auswertungsprofil. Dabei legt die Gültigkeitsdauer des Auswertungsprofiles auch eine zeitliche Zugriffsbegrenzung fest. Es ist deshalb notwendig, dass der GWA eine "profileId" (und "userId") über die Lebensdauer der Messwerte und Anschlussnutzer-Log-Einträge hinweg nur einmalig im SMGW vergibt.

Die Berechtigung zur Nutzung der Proxy-Funktion des SMGW geschieht über ein mit der "profileId" verknüpftes Proxy-Kommunikationsprofil.

Die Berechtigung zum Abruf eines UserLogs geschieht über die "userId".

Die rollenspezifischen Zugriffsrechte auf Daten ("Assets") werden darüber hinaus durch das Schutzprofil des SMGW begrenzt.

Das SMGW erwartet als Aufrufparameter ein HAN-Kommunikationsprofil gemäß ▸Abschnitt 3.22.22. Es prüft die Inhalte des Aufrufparameters und persistiert ein valides übergebenes HAN-Kommunikationsprofil.

Damit bestimmt der GWA organisatorisch über die Zugriffsmöglichkeit eines Anschlussnutzers auf historische Daten innerhalb der Vorhaltefristen, sofern die historischen Messwerte und Logbucheinträge noch im SMGW verfügbar sind.

▸Tabelle 3.36 listet die zulässigen Kombinationen von KS, Rolle und Credentials für die HAN-Kommunikationsprofile auf.

Da die Auswahl des HAN-Kommunikationsprofiles (zur Berechtigungsprüfung und Bestimmung der Rolle) anhand der Credentials bzw. des TLS-Zertifikates des Kommunikationspartners geschieht, muss gewährleistet sein, dass ein HAN-Kommunikationsprofil im SMGW anhand der Credentials und des TLS-Zertifikates eindeutig bestimmt werden kann. Da die Rolle nicht dem Zertifikat entnommen werden kann ist die Eindeutigkeit beim Konfigurieren des HAN-Kommunikationsprofils insbesondere für HKS.WS1 notwendig.

KS	Rolle	Peer-Zertifikat gemäß [DS] Kapitel "Zertifikatsprofile im HAN"	User-Credentials
▸HKS.WS1	CON	CON_HAN_TLS_CRT	Leer
▸HKS.WS1	SRV	CA_SIG_CRT oder SRV_HAN_TLS_CRT	Leer
▸HKS.WS2	CON	Leer	Username/ Password-Hash
▸HKS.WS1	CLS	CLS_HAN_TLS_CRT	Leer
▸HKS.TLSPROXY.CLI, ▸HKS.TLSPROXY.SRV, ▸HKS.TLSPROXY.SOCKS	CLS	CLS_HAN_TLS_CRT	Leer

Tabelle 3.36 Valide Datenfeldkombinationen des HAN-Kommunikationsprofiles

Hinweis: Das HKS.NTP-TLS erfordert keine Authentifizierung und kein HAN-Kommunikationsprofil.

3.13.4.2 Auslöser



REQ.FA.CreateHanUserProfile.100

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.13.4.3 Anforderungen

- Das SMGW **SOLL** die Datenfelder des ▸HAN-Kommunikationsprofil gemäß ▸Tabelle 3.37 auf Plausibilität prüfen und im Fehlerfall den Import ablehnen. ▸ [FNN.20001.2] [REQ.FA.CreateHanUserProfile.10]
- Das SMGW **MUSS** das Anlegen des Kommunikationsprofils ablehnen, falls bereits ein HAN-Kommunikationsprofil mit identischer ▸profileId im SMGW vorliegt. ▸ [FNN.20001.3] [REQ.FA.CreateHanUserProfile.20]
- Das SMGW **MUSS** das HAN-Kommunikationsprofil persistieren und künftig für die Authentifizierung von lokalen Nutzern verwenden. ▸ [FNN.20001.0] [REQ.FA.CreateHanUserProfile.40]

Nr.	Bedingung	Datenfeld	Prüfung
1	▸ks gleich "WS1", "TLSPROXY.CLI", "TLSPROXY.SRV", "TLSPROXY.SOCKS"	▸peerCert	Ist vorhanden, DER-Codiert gemäß [X.690] und entspricht [DS] Kapitel HAN-Zertifikatsprofile mit der Rolle ▸role.

Nr.	Bedingung	Datenfeld	Prüfung
2	▸ks gleich "WS1", "TLSPROXY.CLI", "TLSPROXY.SRV", "TLSPROXY.SOCKS"	▸peerCert	Darf nicht in einem bereits im SMGW konfigurierten HAN-Kommunikationsprofil mit selbem Kommunikationsszenario (▸ks) konfiguriert sein.
3	▸ks gleich "WS1", "TLSPROXY.CLI", "TLSPROXY.SRV", "TLSPROXY.SOCKS"	▸userCredentials	Ist nicht vorhanden.
4	▸ks gleich "TLSPROXY.CLI"	▸outboundConnection	Ist vorhanden.
5	▸ks ungleich "TLSPROXY.CLI"	▸outboundConnection	Ist nicht vorhanden.
6	▸ks gleich "WS2"	▸peerCert	Ist nicht vorhanden.
7	▸ks gleich "WS2"	▸userCredentials	Ist vorhanden.
8	▸ks gleich "WS1" oder "WS2"	▸profileId	Ist innerhalb der Vorhaltefristen der Auswertungsprofile nicht bereits verwendet worden.
9	▸role gleich "CON"	▸userId	Muss vorhanden sein und nicht bereits in einem anderen HAN-Kommunikationsprofil konfiguriert sein.
10	▸role gleich "CON"	▸userCredentials.username	Muss vorhanden sein und nicht bereits in einem anderen HAN-Kommunikationsprofil konfiguriert sein.
11	▸role gleich "CLS"	▸userId	Muss vorhanden sein und nicht bereits in einem anderen HAN-Kommunikationsprofil mit selbem Kommunikationsszenario (▸ks) konfiguriert sein.
12	▸role gleich "SRV"	▸userId	Ist nicht vorhanden.
13	Immer	▸maxSessionDuration	Nicht größer als die in [TR-03109-3] vorgegebene TLS-Sitzungsdauer.
14	▸role gleich "SRV" oder "CLS"	▸maxLogDuration	Das Datenfeld ist nicht vorhanden.
15	▸role gleich "CON"	▸maxLogDuration bewegt sich im Rahmen der ▸ICS.FA.EventLog.40 definierten Zeitdauer.	Das Datenfeld ist nicht vorhanden.

Tabelle 3.37 Plausibilitätsprüfungen

ICS



ICS.FA.CreateHanUserProfile.10

Der GWH **MUSS** im ICS deklarieren, welche Plausibilitätsprüfungen gemäß ▸Tabelle 3.37 das SMGW durchführt.

3.13.5 FA.UpdateHanComProfile

3.13.5.1 Beschreibung

Das SMGW erwartet als Aufrufparameter ein HAN-Kommunikationsprofil gemäß ▸Abschnitt 3.22.22. Das SMGW prüft die Inhalte des Aufrufparameters und aktualisiert bei validem Aufrufparameter Datenfelder eines vorhandenen HAN-Kommunikationsprofiles.

3.13.5.2 Auslöser



REQ.FA.UpdateHanUserProfile.80

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.13.5.3 Anforderungen

- Das SMGW **SOLL** den Import ablehnen, wenn das Profil gemäß ▸Tabelle 3.37 nicht plausibel ist. ▸ [FNN.20003.2] [REQ.FA.UpdateHanUserProfile.10]
- Das SMGW **MUSS** den Import ablehnen, wenn im Profil gemäß ▸Tabelle 3.38 nicht veränderbare Parameter geändert würden ▸ [FNN.20003.3] . [REQ.FA.UpdateHanUserProfile.20]
- Das SMGW **MUSS** für fehlende optionale Datenfelder im Aufrufparameter die entsprechenden bereits konfigurierten Daten unverändert lassen. [REQ.FA.UpdateHanUserProfile.50]
- Sofern das Datenfeld ▸maxLogDuration geändert wird, **MUSS** im Anschlussnutzer-Log protokolliert werden, dass die Vorhaltefrist durch Konfiguration geändert wurde und wie viele Einträge gelöscht wurden. ▸ [BSI.19024.0] [REQ.FA.UpdateHanUserProfile.90]
- Das SMGW **MUSS** das HAN-Kommunikationsprofil persistieren und künftig für die Authentifizierung von lokalen Nutzern verwenden. ▸ [BSI.20003.0] [REQ.FA.UpdateHanUserProfile.40]

Nr.	Bedingung	Datenfeld	Prüfung
1	Immer	▸profileId	Die Profil-Id im Aufrufparameter ist gegenüber dem im SMGW konfigurierten HAN-Kommunikationsprofil nicht geändert.
2	Immer	▸ks	Das Kommunikationsszenario im Aufrufparameter ist gegenüber dem im SMGW konfigurierten HAN-Kommunikationsprofil nicht geändert.
3	Immer	▸role	Die Rolle im Aufrufparameter ist gegenüber dem im SMGW konfigurierten HAN-Kommunikationsprofil nicht geändert.
4	Immer	▸userId	Die "userId" im Aufrufparameter ist gegenüber dem im SMGW konfigurierten HAN-Kommunikationsprofil nicht geändert.

Tabelle 3.38 Plausibilitätsprüfungen

3.13.6 FA.DeleteHanComProfile

3.13.6.1 Beschreibung

Das SMGW löscht das identifizierte HAN-Kommunikationsprofil, so dass der über das HAN-Kommunikationsprofil identifizierte Nutzer keinen Zugriff mehr auf die seiner Rolle zugeordneten Nutzerdaten hat.

Zu beachten ist, dass innerhalb der Gültigkeit und Vorhaltefrist eines Auswertungsprofils zur Gewährleistung der Transparenz für den Endnutzer ein Zugriff auf die Dienste gemäß ▸FAKAT.ConServices möglich sein muss.

3.13.6.2 Auslöser



REQ.FA.DeleteHanUserProfile.30

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.13.6.3 Anforderungen

- Das SMGW **MUSS** das Löschen ablehnen, wenn die referenzielle Integrität gemäß ▸Tabelle 3.39 nicht mehr gegeben wäre. ▸ [FNN.20004.1] [REQ.FA.DeleteHanUserProfile.10]
- Das SMGW **MUSS** das HAN-Kommunikationsprofil im SMGW löschen und künftig nicht mehr für Authentifizierung von lokalen Nutzern am SMGW verwenden. ▸ [FNN.20004.0] [REQ.FA.DeleteHanUserProfile.20]

Nr.	Bedingung	Datenfeld	Prüfung
1	▸role ist gleich "CON"	▸userId	Es existiert kein Auswertungsprofil dessen ▸userId mit der "userId" des zu löschenden HAN-Kommunikationsprofils übereinstimmt und die Vorhaltefrist gemäß ▸Abschnitt 5.5 noch nicht abgelaufen ist.
1	▸role ist gleich "CLS"	▸userId	Es existiert kein Auswertungsprofil dessen ▸clsIds mit der "userId" des zu löschenden HAN-Kommunikationsprofils übereinstimmt.
1	▸role ist gleich "CLS"	▸profileId	Es existiert kein Proxy-Kommunikationsprofil dessen ▸hanPeerRef mit der "profileId" des zu löschenden HAN-Kommunikationsprofils übereinstimmt.

Tabelle 3.39 Plausibilitätsprüfungen

3.13.7 FA.ReadHanComProfile

3.13.7.1 Beschreibung

Das SMGW erwartet als Aufrufparameter die eindeutige Identifikation eines HAN-Kommunikationsprofiles (Siehe ▸Abschnitt 3.22.22) und exportiert dieses an den Aufrufer.

3.13.7.2 Auslöser



REQ.FA.ReadHanUserProfile.20

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle SRV.

3.13.7.3 Anforderungen

Das SMGW **MUSS** das identifizierte HAN-Kommunikationsprofil gemäß ▸Abschnitt 3.22.22 ohne das Datenfeld ▸userCredentials.hash über das auslösende Kommunikationsszenario exportieren. ▸ [BSI.20031.0] [REQ.FA.ReadHanUserProfile.10]

3.13.8 FA.ListIdentifiedCls

3.13.8.1 Beschreibung

Das SMGW exportiert die Liste der Geräte-IDs der im HAN kommunikativ erreichbaren Geräte (CLS) und den Status ihrer kommunikativen Anbindung.

Dieser FA unterstützt GWA und Servicetechniker bei der Diagnose zur kommunikativen Anbindung von CLS an das SMGW.

Folgende Zustände werden bei der Auflistung der kommunikativ erreichbaren CLS unterschieden:

- PROFILE_ONLY: kennzeichnet den Zustand, wenn ein HAN-Kommunikationsprofil konfiguriert ist, ohne dass das CLS im Netzwerk identifiziert wurde.
- IDENTIFIED: kennzeichnet den Zustand, wenn ein CLS auf eine ▸HKS.DNSDISCOVERY (mDNS)-Anfrage geantwortet hat und noch kein Pairing über den Kommunikationsschlüssel (Zertifikat) erfolgt ist. Da das CLS nicht authentifiziert ist, kann die Lebensdauer dieser Listeneinträge begrenzt werden.
- AUTHENTICATED: kennzeichnet den Zustand, wenn das Pairing mit dem initialen Gerätezertifikat (CLS_HAN_TLS_CRT_0) erfolgt ist aber noch keine Anwendungsdatenkommunikation stattgefunden hat.
- DATA_EXCHANGE: kennzeichnet den Zustand, wenn mindestens eine empfangene Anwendungsnachricht erfolgreich entschlüsselt wurde (HKS.WS1 Request oder TLS-Proxy-Datentransfer).

Die Semantik der bereitgestellten Informationen ist wie folgt:

- ▸cls.l2Address enthält die Ethernet MAC-Adresse des CLS
- ▸cls.ipv4Address enthält die (link-lokale) IPv4-Adresse des CLS
- ▸cls.ipv6Address enthält die (link-lokale) IPv6-Adresse des CLS
- ▸cls.clsId enthält die mittels ▸HKS.DNSDISCOVERY ermittelte bzw. im Kommunikationsprofil konfigurierte eindeutige Geräteidentifikation des CLS.
- ▸cls.services enthält die mittels ▸HKS.DNSDISCOVERY (DNS-SD SRV-Records) ermittelten Port-Nummern und Dienste des CLS.
- ▸cls.additionalInfos enthält die mittels ▸HKS.DNSDISCOVERY (DNS-SD TXT-Records) ermittelten Geräteinformationen des CLS.

Die Aufzeichnung des letzten Empfangszeitpunktes einer (Layer 2-)Nachricht des Gerätes ermöglicht die zeitliche Zuordnung zu physischen Ereignissen, die zu Übertragungsstörungen führen.

3.13.8.2 Auslöser



REQ.FA.ListIdentifiedCls.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT von der Rolle GWA.
- Empfang einer Anfrage über ▸HKS.WS1 von der Rolle SRV.

3.13.8.3 Anforderungen

- Das SMGW **MUSS** die im SMGW identifizierten und sichtbaren CLS für den Aufrufer mit der Datenstruktur ▸Abschnitt 3.22.12 auflisten. [REQ.FA.ListIdentifiedCls.20]
- Das SMGW **MUSS** das Datenfeld ▸cls.lastTs auf den Zeitpunkt des letzten Empfangs eines IP-Pakets vom CLS setzen. [REQ.FA.ListIdentifiedCls.30]
- Das SMGW **MUSS** das Datenfeld ▸cls.pairingState gemäß ▸Tabelle 3.40 setzen. [REQ.FA.ListIdentifiedCls.40]
- Das SMGW **SOLL** Listeneinträge im Zustand "IDENTIFIED" nach festgelegter Zeit entfernen (▸ICS.FA.ListIdentifiedCls.10). [REQ.FA.ListIdentifiedCls.50]

Datenfeld ▸cls.pairingState	Bedeutung
PROFILE_ONLY	Ein Kommunikationsprofil für das CLS ist konfiguriert. Das CLS wurde noch nicht im HAN identifiziert. D.h. es wurde noch keine Nachricht (Layer 2/3) vom CLS empfangen.
IDENTIFIED	Das CLS wurde im HAN identifiziert, d.h. es wurde eine Nachricht (Layer 2/3) vom CLS empfangen; allerdings ist noch kein Pairing über das initiale CLS_HAN_TLS_CRT_0 erfolgt. Dieser Zustand kann auch eintreten, wenn noch kein Kommunikationsprofil konfiguriert ist.
AUTHENTICATED	Das Pairing mit dem initialen CLS_HAN_TLS_CRT_0 ist erfolgt, aber es wurde noch keine Anwendungsnachricht verarbeitet.
DATA_EXCHANGE	Mindestens eine Anwendungsnachricht wurde erfolgreich verarbeitet.

Tabelle 3.40 Bedeutung des Pairing-State des CLS

ICS



ICS.FA.ListIdentifiedCls.10

Der GWH **MUSS** im ICS angeben, nach welcher Zeit (in Minuten, aufgerundet) identifizierte, aber nicht authentifizierte CLS (IDENTIFIED) aus der Liste entfernt werden. Der Wert 0 gibt an, dass CLS nicht automatisch aus der Liste entfernt werden.

3.14 Messwertverarbeitung administrieren (FAKAT.ValProcConfig)

3.14.1 Übersicht

Die Messwertverarbeitung ist verantwortlich für den Empfang, die Verarbeitung und den Versand von Messwerten. Die regelbasierte Verarbeitung und die zulässigen Datenflüsse zwischen den Schnittstellen des SMGW zu den Netzen LMN, HAN, WAN werden durch Auswertungsprofile (engl. Processing Profiles) durch den GWA konfiguriert. Die kommunikative Anbindung von Messeinrichtungen, Anschlussnutzern und EMT wird in den FA-Kategorien ▸FAKAT.LmnComConfig, ▸FAKAT.HanUserConfig und ▸FAKAT.EmtComConfig beschrieben.

▸Abbildung 3.18 zeigt die Relationen der über Datenfelder identifizierten Entitäten der in die Messwertverarbeitung involvierten Entitäten (Datenobjekte und Akteure) des SMGW.

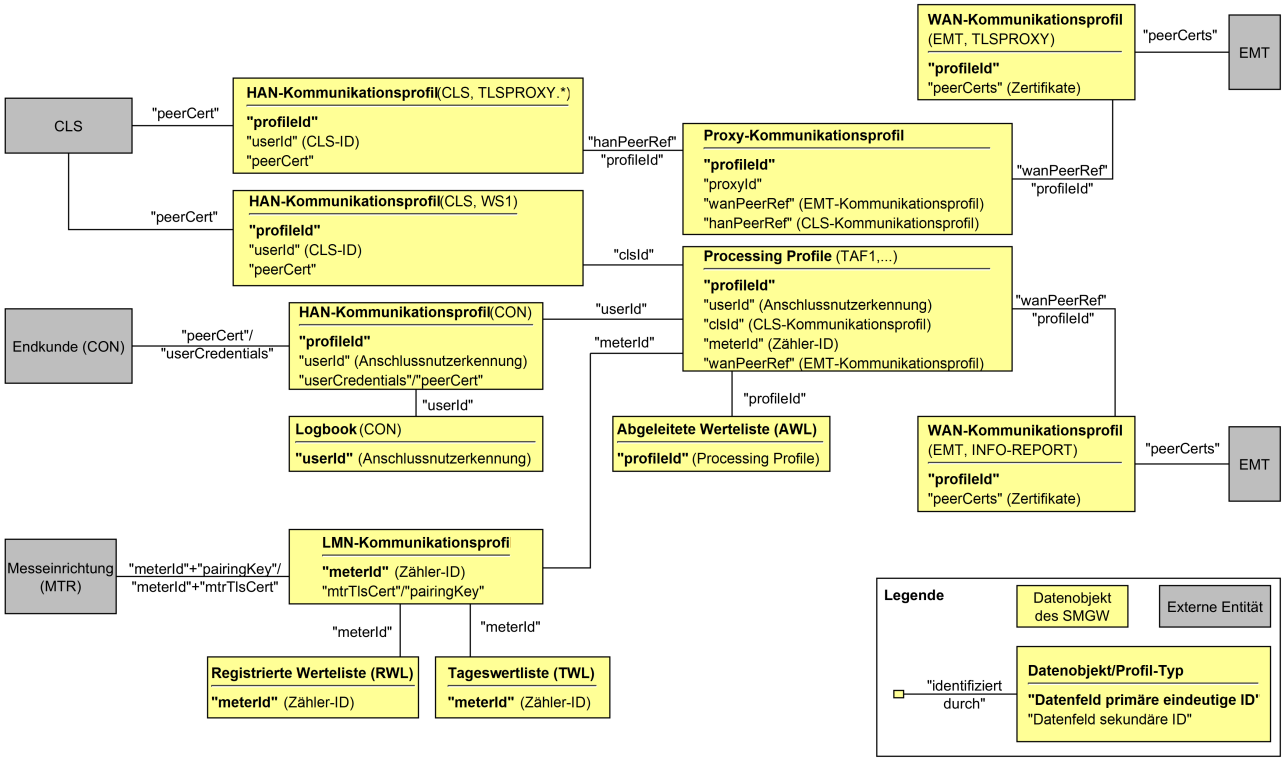


Abbildung 3.18. Relationen zwischen Entitäten der Messwertverarbeitung des SMGW

Nicht dargestellt ist die zeitliche Dimension im Lebenszyklus der Entitäten: Zugriffsberechtigungen auf historische Wertelisten, die sich durch "meterId", "userId" ergeben, sind über den Gültigkeitszeitraum des Auswertungsprofiles eingeschränkt.

Das SMGW setzt die FAs gemäß ▸Tabelle 3.41 um.

3.14.2 Übersicht der FA

Aufgabe	FA
Konfiguration eines neuen Auswertungsprofils importieren	Das SMGW **MUSS** ▸FA.CreateProcessingProfile für den GWA umsetzen. [REQ.FAKAT.MeteringConfig.10]
Konfiguration eines eingespielten Auswertungsprofils ändern	Das SMGW **SOLL** ▸FA.UpdateProcessingProfile für den GWA umsetzen. [REQ.FAKAT.MeteringConfig.20]
Konfiguration eines Auswertungsprofils löschen	Das SMGW **MUSS** ▸FA.DeleteProcessingProfile für den GWA umsetzen. [REQ.FAKAT.MeteringConfig.30]
Konfiguration eines Auswertungsprofils auslesen	Das SMGW **MUSS** ▸FA.ReadProcessingProfile für den GWA umsetzen. [REQ.FAKAT.MeteringConfig.50]

Tabelle 3.41 Übersicht der FA der Kategorie FAKAT.ValProcConfig

3.14.3 Datenstrukturen der FA-Kategorie

Das Auswertungsprofil ist in ▸Abschnitt 3.22.6 beschrieben.

Die Datenstruktur mit den Aufrufparametern für die Bedarfsauslesung sind in ▸Abschnitt 3.22.34 beschrieben.

3.14.4 FA.CreateProcessingProfile

3.14.4.1 Beschreibung

Dieser FA beschreibt die Funktionalität, ein neues Auswertungsprofil gemäß ▸Abschnitt 3.22.6 zu importieren.

Das SMGW prüft die für die jeweiligen TAF zulässigen Inhalte der zu importierenden Datenfelder und weist ungültige Kombinationen zurück. Zwischen Beginn und Ende der Gültigkeit des Auswertungsprofiles empfängt, speichert, verarbeitet und versendet das SMGW gemäß Regelwerk die Messwerte.

Jedes Auswertungsprofil ist genau einer Messeinrichtung mit der Identifikation ▸meterReadingInput.meterId zugeordnet, die zuvor administrativ über ein LMN-Kommunikationsprofil mit dem SMGW verknüpft wurde.

Jedes Auswertungsprofil ist genau einem Anschlussnutzer mit der Identifikation ▸userId zugeordnet.

Jedes Auswertungsprofil ist genau einem EMT über ▸meterDataOutput.wanPeerRef zugeordnet, dessen kommunikative Anbindung über ein EMT-WAN-Kommunikationsprofil vom Typ INFO-REPORT angelegt wurde. Es können mehrere Auswertungsprofile mit gleicher ▸meterDataOutput.wanPeerRef im SMGW konfiguriert sein.

An die für Abrechnungszwecke verwendbaren Auswertungsprofile (▸TAF1, ▸TAF2, ▸TAF7, ▸TAF8, ▸TAF15) werden Import-Anforderungen an die zulässige Registrierperiode, die zulässigen Messgrößen-Identifikationen der Register bei Erfassung und Versand gestellt.

Die Konfiguration der Registrierperiode für elektrische Energiezählerstände ist auf 15 Minuten festgelegt. Für Zähler anderer Sparten ist es Aufgabe des GWA, eine Registrierperiode zu wählen, die über die Lebensdauer der dem Zähler zugeordneten RWL nicht verändert werden muss.

3.14.4.2 Auslöser



REQ.FA.CreateProcessingProfile.260

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.14.4.3 Anforderungen

- Das SMGW führt für das zu importierende Auswertungsprofil folgende Prüfungen durch. Die Reihenfolge der Prüfungen ist dabei nicht vorgegeben.
  - Das SMGW **MUSS** den Import ablehnen, sofern das per ▸meterReadingInput.meterId referenzierte LMN-Kommunikationsprofil nicht im SMGW konfiguriert ist. ▸ [FNN.20010.3] [REQ.FA.CreateProcessingProfile.10]
  - Das SMGW **MUSS** den Import ablehnen, wenn kein EMT-WAN-Kommunikationsprofil vom Typ INFO-REPORT konfiguriert ist, dessen Profil-Id dem Wert des Datenfeldes ▸meterDataOutput.wanPeerRef entspricht. ▸ [FNN.20010.4] [REQ.FA.CreateProcessingProfile.30]
  - Das SMGW **SOLL** die Datenfelder gemäß ▸Tabelle 3.42 auf Plausibilität prüfen und im Fehlerfall den Import ablehnen. ▸ [FNN.20010.7] [REQ.FA.CreateProcessingProfile.15]
- Das SMGW **MUSS** das Auswertungsprofil so persistieren, das von Beginn bis Ende des Gültigkeitszeitraumes über das über ▸meterReadingInput.meterId verknüpfte LMN-Kommunikationsprofil Messwerte erfasst und verarbeitet werden, über das mittels ▸userId verknüpfte HAN-Kommunikationsprofil autorisierte Messwerte abgerufen werden können und über das mittels ▸meterDataOutput.wanPeerRef verknüpfte WAN-Kommunikationsprofil Messwerte versandt werden. [REQ.FA.CreateProcessingProfile.60]

- Das SMGW **MUSS** die Messwertverarbeitung des Auswertungsprofils zu Beginn des *Gültigkeitszeitraums* oder, falls der Beginn des Gültigkeitszeitraums in der Vergangenheit liegt, zum Zeitpunkt des Einspielens aufnehmen. [REQ.FA.CreateProcessingProfile.50] Zur Erstauslesung siehe ▸REQ.FA.ExportAccntMtrReading.10.
- Das SMGW **MUSS** die Messwertverarbeitung des Auswertungsprofils zum Ende des Gültigkeitszeitraums ▸validityPeriod einstellen. [REQ.FA.CreateProcessingProfile.70] Zur Schlussauslesung siehe ▸REQ.FA.ExportAccntMtrReading.10.
- Das SMGW **MUSS** den Inhalt der Datenfelder ▸meterReadingInput, ▸userId, ▸meterDataOutput.wanPeerRef, ▸tafType, ▸validityPeriod und für die abrechnungsrelevanten TAF die "tafNParameter" im Eichtechnischen Log und über das Datenfeld ▸userId zugeordneten Anschlussnutzer-Log protokollieren. ▸[BSI.20010.0] [REQ.WFA.EichlogInhalt.40]

Nr.	Bedingung	Datenfeld	Prüfung
1	Immer	▸tafId	Es darf noch kein Auswertungsprofil mit gleicher ▸tafId im SMGW konfiguriert sein.
2	▸tafType gleich ▸TAF1 und es existiert bereits eine ▸RWL für ▸meterReadingInput.meterId	▸taf1Params.regInterval	Muss mit den Intervall der Zählerstände in der existierenden ▸RWL übereinstimmen.
3	▸tafType gleich ▸TAF2 und es existiert bereits eine ▸RWL für ▸meterReadingInput.meterId	▸taf2Params.regInterval	Muss mit den Intervall der Zählerstände in der existierenden ▸RWL übereinstimmen.
4	▸tafType gleich ▸TAF7 und es existiert bereits eine ▸RWL für ▸meterReadingInput.meterId	▸taf7Params.regInterval	Muss mit den Intervall der Zählerstände in der existierenden ▸RWL übereinstimmen.
5	▸tafType gleich ▸TAF8 und es existiert bereits eine ▸RWL für ▸meterReadingInput.meterId	▸taf8Params.regInterval	Muss mit den Intervall der Zählerstände in der existierenden ▸RWL übereinstimmen.
6	▸tafType gleich ▸TAF1	▸meterReadingInput.obis	Im Datenfeld ▸meterReadingInput.obis muss genau eine Kennzahl konfiguriert sein.
7	Immer	▸meterReadingInput.obis	Die OBIS-IDs in ▸meterReadingInput.obis müssen gemäß ▸Tabelle 3.43 für die Messwertverarbeitung des ▸tafType zulässig sein.
8	Immer	▸taf9Params.capPeriod, ▸taf10Params.capPeriod bzw. ▸taf14Params.capPeriod	Der Wert muss 0 oder größer gleich ▸ICS.FA.CreateProcessingProfile.30 sein.
9	▸tafType gleich ▸TAF9, ▸TAF10, ▸TAF14	▸signMode	Muss gleich "NONE" sein, d.h. die Exportierten Werte werden nicht signiert.
10	Nicht vorhanden		
11	Immer	"*tafN*Params"	Es muss genau ein Datenfeld "*tafN*Params" angegeben sein und dieses muss dem ▸tafType entsprechen.
12	Immer	▸validityPeriod.to	Das Ende des Gültigkeitszeitraumes muss bezüglich der Systemzeit in der Zukunft liegen
13	Immer	▸validityPeriod.to	Das Ende des Gültigkeitszeitraumes muss nach dem Beginn des Gültigkeitszeitraumes ▸validityPeriod.from liegen.

Nr.	Bedingung	Datenfeld	Prüfung
14	▸tafType gleich ▸TAF1, ▸TAF2, ▸TAF7 und ▸meterReadingInput.obis enthält eine OBIS-Kennzahl für elektrische Energie (Value Group A=1)	▸taf1Params.regInterval, ▸taf2Params.regInterval oder ▸taf7Params.regInterval	Die Registrierperiode darf nicht größer als "QUARTER_HOURLY" sein.
15	▸tafType gleich ▸TAF8, ▸TAF15 und ▸meterReadingInput.obis enthält eine OBIS-Kennzahl für elektrische Energie (Value Group A=1)	▸taf8Params.regInterval, oder ▸taf15Params.regInterval	Die Registrierperiode darf nicht größer als "QUARTER_HOURLY" sein.
16	▸tafType gleich ▸TAF2, ▸TAF7, ▸TAF8 oder ▸TAF15	▸meterDataOutput.trigger.deliveryTime	Es muss ein Versandauslösezeitpunkt angegeben sein.
17	▸tafType gleich ▸TAF1, ▸TAF2, ▸TAF7, ▸TAF8, ▸TAF15"	▸validityPeriod.from und ▸validityPeriod.to	Die Zeitpunkte sollen auf einem Sollregistrierzeitpunkt (siehe ▸Abschnitt 3.2.4.2) gemäß Registrierperiode des Auswertungsprofils fallen.
18	▸tafType nicht gleich ▸TAF9, ▸TAF10, ▸TAF14	▸meterDataOutput.trigger.thresholds	Darf nicht angegeben sein.
19	▸tafType gleich ▸TAF1	▸meterDataOutput.trigger.deliveryTime.day	Das Datenfeld muss vorhanden sein.
20	▸tafType gleich ▸TAF7, ▸TAF2, ▸TAF8 oder ▸TAF15	▸meterDataOutput.trigger.deliveryTime	Das Datenfeld muss vorhanden sein.
21	Immer	▸meterDataOutput.trigger	Es darf höchstens eine Art von Versandauslöser (▸meterDataOutput.trigger.deliveryTime oder ▸meterDataOutput.trigger.thresholds) vorhanden sein.
22	▸ICS.FAKAT.ValProcBilling.20 gleich "false"	▸tafType	Darf nicht gleich TAF15 sein.
23	Immer	▸userId	Es ist ein HAN-Kommunikationsprofil konfiguriert, das eindeutig vom Auswertungsprofil referenziert werden kann (▸userId gleich ▸userId).
24	▸tafType gleich ▸TAF7 und ▸meterReadingInput.obis enthält eine OBIS-Kennzahl für Gas (Value Group A=7)	▸taf7Params.regInterval	Die Registrierperiode muss "HOURLY" sein.
25	Nicht vorhanden		
26	Immer	▸meterReadingInput.obis	Die Messgröße kann gemäß ▸supportedValues von der Messeinrichtung bereitgestellt werden.
27	Es ist eine Registrierperiodenlänge von 5 Minuten angegeben	▸taf1Params.regInterval, ▸taf2Params.regInterval, ▸taf7Params.regInterval, ▸taf8Params.regInterval oder ▸taf15Params.regInterval	Das SMGW unterstützt für den gewählten TAF eine 5 minütliche Registrierung nach ▸ICS.FA.CreateProcessingProfile.50

Tabelle 3.42 Plausibilitätsprüfungen

Eingangsmesswert (OBIS)	Eingangsmessgröße	Verarbeitung	Bereitgestellte Werte (OBIS)
▸TAF1			
1-0:C.8.0*255	Zählerstand Elektrische Energie (C=1, 2, 5, 6, 7, 8)	Registrierung Zählerstand	1-0:C.8.0*255 (Zählerstand)
7-0:3.D.0*255	Zählerstand Gas Volumen (D=0, 1)	Registrierung Zählerstand	7-0:3.D.0*255 (Zählerstand)
7-0:13.2.0*255	Umwerterstand Gas Volumen	Registrierung Zählerstand	7-0:13.2.0*255 (Zählerstand)

Eingangsmesswert (OBIS)	Eingangsmessgröße	Verarbeitung	Bereitgestellte Werte (OBIS)
A-0:1.0.0*255	Zählerstand Thermische Energie und Wasservolumen (A=4, 5, 6, 7, 8)	Registrierung Zählerstand	A-0:1.0.0*255 (Zählerstand)
TAF2			
1-0:C.8.0*255	Zählerstand Elektrische Energie (C=1, 2, 5, 6, 7, 8)	Registrierung Zählerstand, Register für zeitvariablen Tarif	1-0:C.9.E*255 (Tarifstufenregister) (deprecated TAF2: 1-0:C.8.E*255)
TAF7			
1-0:C.8.0*255	Zählerstand Elektrische Energie (C=1, 2, 5, 6, 7, 8)	Registrierung Zählerstand	1-0:C.8.0*255 (Zählerstand)
7-0:3.D.0*255	Zählerstand Gas Volumen (D=0, 1)	Registrierung Zählerstand	7-0:3.D.0*255 (Zählerstand)
7-0:13.2.0*255	Umwerterstand Gas Volumen	Registrierung Zählerstand	7-0:13.2.0*255 (Zählerstand)
7-0:C.D.0*255	Zustand Gas Temperatur (C=41) / Druck (C=42), (D=0, 2)	Erfassung Momentanwert	7-0:C.D.0*255 (Momentanwert)
A-0:1.0.0*255	Zählerstand Thermische Energie und Wasservolumen (A=4, 5, 6, 7, 8)	Registrierung Zählerstand	A-0:1.0.0*255 (Zählerstand)
TAF8			
1-0:C.8.0*255	Zählerstand Elektrische Energie (C=1, 2, 5, 6, 7, 8)	Registrierung Zählerstand, Ableitung mittlere Leistung, Maximumbildung	1-0:C.8.0*255 (Zählerstand) 1-0:C.29.0 (Lastgang) 1-0:C.6.0 (Maximum)
TAF9			
1-0:C.7.0*255	Momentanwert Wirkleistung (C=16, 36, 56, 76)	Erfassung Momentanwert	Wie Eingangsmesswerte
TAF10			
1-0:C.7.0*255	Momentanwert Wirkleistung (C=16, 36, 56, 76), Spannung, Strom, Frequenz (C=32, 52, 72, 31, 51, 71, 14)	Erfassung Momentanwert	Wie Eingangsmesswerte
1-0:81.7.E*255	Momentanwert Phasenwinkel (E=1, 2, 4, 15, 26)	Erfassung Momentanwert	Wie Eingangsmesswerte
A-0:C.D.E*F	A-F gemäß ▸ICS.MWV.Taf14Obis.10	Erfassung Momentanwert	Wie Eingangsmesswerte
TAF14			
1-0:C.8.0*255	Zählerstand Elektrische Energie (C=1, 21, 41, 61, 2, 22, 42, 62, 5, 6, 7, 8)	Erfassung Momentanwert	Wie Eingangsmesswerte
1-0:C.7.0*255	Momentanwert Wirkleistung (C=16, 36, 56, 76)	Erfassung Momentanwert	Wie Eingangsmesswerte
A-0:C.D.E*F	A-F gemäß ▸ICS.MWV.Taf14Obis.10	Erfassung Momentanwert	Wie Eingangsmesswerte
TAF15			
1-0:C.D.E*255	Elektrische Energie Messwerte	Erfassung registrierter Messwerte	Wie Eingangsmesswerte
7-0:C.D.E*255	Gas Messwerte	Erfassung registrierter Messwerte	Wie Eingangsmesswerte

Tabelle 3.43 Für die Verarbeitung zugelassene identifizierte Messgrößen

ICS



ICS.MWV.Taf14Obis.10

Der GWH **MUSS** im ICS angeben, welche OBIS-Kennzahlen das SMGW bei der Konfiguration, Erfassung und Versand von Messwerten zusätzlich zu ▸Tabelle 3.43 für ▸TAF10 und ▸TAF14 unterstützt.



ICS.FA.CreateProcessingProfile.30

Der GWH **MUSS** im ICS angeben, welche kleinste Messwertabfrage- und Erfassungsperiode das SMGW unterstützt. Der Wert muss zwischen 1 und 60 Sekunden liegen.



ICS.FA.CreateProcessingProfile.40

Der GWH **MUSS** im ICS deklarieren, welche Plausibilitätsprüfungen gemäß ▸Tabelle 3.42 das SMGW durchführt. Werden Plausibilitätsprüfungen nicht durch das SMGW durchgeführt, ist in einer Verwenderauflage zu beschreiben, dass dies vom GWA durchgeführt werden muss.



ICS.FA.CreateProcessingProfile.50

Der GWH **MUSS** im ICS deklarieren, ob und für welche TAF das SMGW eine Registrierperiode von 5 Minuten unterstützt. Hierbei ist zu beachten, dass eine 5 minütliche Registrierung im SMGW entsprechende Anforderungen an die Zeitsynchronisation stellt (vgl. ▸ICS.FA.TimeSyncWithGwa.80).

3.14.4.4 Implementierungshinweise

Eine rückwirkende Tarifierung bei abrechnungsrelevanten TAF ist bei einem neu eingespielten Auswertungsprofil mit einem in der Vergangenheit liegenden Beginn des Gültigkeitszeitraums ▸validityPeriod auszuschließen. Auch bei einer sofortigen Aufnahme des Betriebs des Regelwerks ist das Raster, das durch die Registrierperiode vorgegeben wird, einzuhalten (siehe *Sollregistrierzeitpunkt*).

3.14.5 FA.UpdateProcessingProfile

3.14.5.1 Beschreibung

Dieser FA beschreibt die Funktionalität zur Änderung eines Auswertungsprofils. Der Umfang, indem ein Auswertungsprofil geändert werden kann, ist abhängig vom verwendeten TAF und dessen Gültigkeitszeitraums:

- Während und vor Beginn des Gültigkeitszeitraumes können nur der Endzeitpunkt des Gültigkeitszeitraums (▸validityPeriod.to) und die Versandzeitpunkte (▸meterDataOutput.trigger) geändert werden. Wenige weitere Änderungen sind TAF-spezifisch, wie unten beschrieben, möglich.
- Sollte eine Änderung an anderen Parametern notwendig sein, muss das Auswertungsprofil gelöscht und ein neues Auswertungsprofil eingespielt werden.
- Nach Ablauf des Gültigkeitszeitraums sind keine Änderungen des Auswertungsprofils mehr möglich.

3.14.5.2 Auslöser



REQ.FA.UpdateProcessingProfile.90

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.14.5.3 Anforderungen

- Wenn das zu ändernde Auswertungsprofil zu einem TAF gehört, dessen Gültigkeitszeitraum bereits abgelaufen ist, **MUSS** das SMGW die Änderung ablehnen. [REQ.FA.UpdateProcessingProfile.60]
- Wenn das zu ändernde Auswertungsprofil zu einem TAF gehört, dessen Gültigkeitszeitraum noch nicht abgelaufen ist **MUSS** das SMGW Änderungen von Datenfeldern ablehnen, wenn sie nicht als TAF-spezifische Ausnahme in ▸Tabelle 3.44 aufgeführt sind. ▸ [FNN.20011.6] [REQ.FA.UpdateProcessingProfile.20]

- Das SMGW **SOLL** den Import ablehnen, wenn das Profil gemäß ▸Tabelle 3.42 nicht plausibel und eindeutig ist. ▸ [FNN.20011.5] [REQ.FA.UpdateProcessingProfile.15]
- Das SMGW **MUSS** die Änderungen des Auswertungsprofil persistieren. [REQ.FA.UpdateProcessingProfile.80]
- Das SMGW **MUSS** den Inhalt der geänderten Datenfelder "validityPeriod" im Eichtechnischen Log und dem "userId" zugeordneten Anschlussnutzer-Log protokollieren. ▸ [PTB.20011.0] ▸ [PTB.20032.0] [REQ.WFA.EichlogInhalt.41]

Parameter	Bedingungen
Alle TAF	
▸validityPeriod.to	Das bisher konfigurierte ▸validityPeriod.to liegt in Zukunft oder wurde noch nicht definiert.
▸meterDataOutput.trigger	Einschließlich aller Unterparameter unter Berücksichtigung der Anforderungen aus ▸FA.CreateProcessingProfile
▸clsIds	Änderung immer zulässig.
▸TAF2	
▸taf2Params.timeOfUseDefinition	Einschließlich aller Unterparameter jedoch nur die Tupel, deren Zeitpunkt ▸taf2Params.timeOfUseDefinition.time nach dem nächsten Sollregistrierzeitpunkt liegt.
▸TAF9, ▸TAF10, ▸TAF14	
▸meterReadingInput.obis	Unter Berücksichtigung der Anforderungen aus ▸FA.CreateProcessingProfile.
▸meterDataOutput.trigger.thresholds	Einschließlich aller Unterparameter unter Berücksichtigung der Anforderungen aus ▸FA.CreateProcessingProfile.

Tabelle 3.44 Veränderbare Datenfelder

3.14.6 FA.DeleteProcessingProfile

3.14.6.1 Beschreibung

Dieser FA beschreibt die Funktionalität zur Löschung eines Auswertungsprofils. Da das Auswertungsprofil den Anschlussnutzer mit einer Messeinrichtung und deren RWL und AWL verknüpft, entfällt dadurch der Zugriff auf diese Daten. Der EMT erhält keine Messwerte mehr und das SMGW erfasst für dieses Auswertungsprofil keine Messwerte mehr.

Sofern der GWA diesen FA aufruft, berücksichtigt er beim Löschen der abrechnungsrelevanten Auswertungsprofile die Vorhaltefrist (siehe ▸Abschnitt 5.5).

Der Gültigkeitszeitraumes kann mit ▸FA.UpdateProcessingProfile verkürzt werden, um den Löschzeitpunkt vorzuziehen.

3.14.6.2 Auslöser



REQ.FA.DeleteProcessingProfile.40

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- ▸tafState gleich "archived" und ▸autoCleanUp gleich "true" und Systemzeit überschreitet den Tageswechsel nach ▸validityPeriod.to + ▸archiveDuration.

3.14.6.3 Anforderungen

- (tafType gleich "TAF1", "TAF2", "TAF7", "TAF8", "TAF15") Das SMGW **MUSS** das Löschen ablehnen, wenn ▸tafState gleich "running" ist. ▸ [FNN.20013.3] [REQ.FA.DeleteProcessingProfile.10]

- (tafType gleich "TAF1", "TAF2", "TAF7", "TAF8", "TAF15") Das SMGW **MUSS** das Löschen ablehnen, wenn der Zeitpunkt ▸validityPeriod.to + ▸Abschnitt 5.5 nicht erreicht ist. ▸ [FNN.20013.1] [REQ.FA.DeleteProcessingProfile.20]



REQ.FA.DeleteProcessingProfile.30

Das SMGW **MUSS** das persistierte Auswertungsprofil so löschen, dass

- in der über die ▸meterReadingInput.meterId verknüpften ▸TWL, ▸AWL, ▸RWL und ▸NWL gemäß dieses Auswertungsprofiles keine Messwerte registriert oder erfasst werden,
- über ein mit ▸userId verknüpftem HAN-Kommunikationsprofil kein Zugriff auf die mit ▸meterReadingInput.meterId verknüpften ▸TWL, ▸AWL, ▸RWL und ▸NWL möglich ist,
- über ein mit ▸clsIds verknüpftem HAN-Kommunikationsprofil kein Zugriff auf die mit ▸meterReadingInput.meterId verknüpften ▸TWL, ▸AWL, ▸RWL und ▸NWL möglich ist,
- über die mit ▸meterDataOutput.wanPeerRef verknüpften WAN-Kommunikationsprofile (INFO-REPORT) kein Versand durch dieses Auswertungsprofil ausgelöst wird.

▸ [BSI.20013.0]

3.14.6.4 Implementierungshinweise

Sollte das Auswertungsprofil eines nicht-abrechnungsrelevanten TAF gelöscht werden, wird empfohlen, den TAF mit Zeitpunkt der Löschung zu beenden.

Der Versand der Messwerte zum Ende des Gültigkeitszeitraumes wird über ▸FA.ExportAccntMtrReading ausgelöst.

Ob die Messwerte der ▸RWL oder ▸NWL gelöscht werden können hängt davon ab, ob noch weitere Auswertungsprofile Zugriff auf die mit der Messeinrichtung verknüpften Messwerte benötigen.

3.14.7 FA.ReadProcessingProfile

3.14.7.1 Beschreibung

Dieser FA erlaubt das Auslesen eingespielter Auswertungsprofile. Nur der GWA, sowie der im Auswertungsprofil über das HAN-Kommunikationsprofil zugeordnete Anschlussnutzer oder CLS kann das Auswertungsprofil auslesen (Siehe ▸Anhang C).

3.14.7.2 Auslöser



REQ.FA.ReadProcessingProfile.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle CON oder CLS.
- Empfang einer Anfrage über ▸HKS.WS2.

3.14.7.3 Anforderungen

- Das SMGW **MUSS** das in der Anfrage angeforderte Auswertungsprofil gemäß ▸Abschnitt 3.22.6 an den Aufrufer ausliefern. [REQ.FA.ReadProcessingProfile.20]

3.15 Proxy-Kommunikation administrieren (FAKAT.ProxyConfig)

3.15.1 Übersicht

Die Anwendungsfälle dieser Kategorie ermöglichen dem GWA die Administration und Konfiguration der Proxy-Funktion des SMGW, um einen über das SMGW vermittelten Datenaustausch zwischen CLS und aktivem EMT im WAN zu unterstützen.

3.15.2 Übersicht der FA

Aufgabe	Umsetzung
Konfiguration zur Vermittlung von Proxy-Kommunikationsverbindungen durch GWA importieren	Das SMGW **MUSS** ▸FA.CreateProxyComProfile für den GWA umsetzen. [REQ.WAN.Management.80] Ergänzend siehe auch ▸FA.CreateWanComProfile für aEMT und ▸FA.CreateHanComProfile für CLS
Konfiguration zur Vermittlung von Proxy-Kommunikationsverbindungen durch GWA aktualisieren	Das SMGW **MUSS** ▸FA.UpdateProxyComProfile für den GWA umsetzen. [REQ.WAN.Management.81] Ergänzend siehe auch ▸FA.UpdateWanComProfile für aEMT und ▸FA.UpdateHanComProfile für CLS
Konfiguration zur Vermittlung von Proxy-Kommunikationsverbindungen durch GWA löschen	Das SMGW **MUSS** ▸FA.DeleteProxyComProfile für den GWA umsetzen. [REQ.WAN.Management.90] Ergänzend siehe auch ▸FA.DeleteWanComProfile für aEMT und ▸FA.DeleteHanComProfile für CLS
Konfiguration zur Vermittlung von Proxy-Kommunikationsverbindungen durch GWA auslesen	Das SMGW **MUSS** ▸FA.ReadProxyComProfile für den GWA umsetzen. [REQ.FAKAT.ProxyConfig.20] Ergänzend siehe auch ▸FA.ReadWanComProfile für aEMT und ▸FA.ReadHanComProfile für CLS
Zustand eines Proxy-Kommunikationskanals durch den GWA abfragen	Das SMGW **SOLL** ▸FA.ReadProxyChStatus für den GWA umsetzen. [REQ.FAKAT.ProxyConfig.30]

Tabelle 3.45 Übersicht der FA der Kategorie FAKAT.ProxyConfig

ICS



ICS.FAKAT.ProxyConfig.10

Der GWH **MUSS** im ICS deklarieren, ob das SMGW dem GWA ▸FA.ReadProxyChStatus bereitstellt.

3.15.3 Datenstrukturen der FA-Kategorie

Das Proxy-Kommunikationsprofil ist in ▸Abschnitt 3.22.37 beschrieben.

Die Datenstruktur mit den Proxy-Statusinformationen ist in ▸Abschnitt 3.22.38 beschrieben.

3.15.4 FA.CreateProxyComProfile

3.15.4.1 Beschreibung

Das SMGW prüft und persistiert ein als Aufrufparameter übermitteltes Proxy-Kommunikationsprofil (▸Proxy-Kommunikationsprofil), das die Parameter zur Vermittlung von Proxy-Kommunikationsverbindungen zwischen CLS und aEMT enthält. Für das CLS muss ein HAN-Kommunikationsprofil konfiguriert sein, für den EMT muss ein WAN-Kommunikationsprofil vom Typ "TLSPROXY" konfiguriert sein.

Für einen aEMT können mehrere Proxy-Kommunikationsprofile konfiguriert werden, sofern das Kommunikationssystem des EMT anhand der Adresse, dem ▸localServerName die ankommende Verbindung unterscheiden und einem Proxy-Kanal zuordnen kann.

3.15.4.2 Auslöser



REQ.FA.CreateProxyConfig.100

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.15.4.3 Anforderungen

- Das SMGW **MUSS** den Import ablehnen, wenn bereits ein Proxy-Kommunikationsprofil mit identischer ▸profileId konfiguriert ist. ▸ [FNN.20014.4] [REQ.FA.CreateProxyConfig.10]

- Das SMGW **MUSS** den Import ablehnen, wenn das über ▸wanPeerRef referenzierte WAN-Kommunikationsprofil nicht im SMGW konfiguriert ist. ▸ [FNN.20014.2] [REQ.FA.CreateProxyConfig.15]
- Das SMGW **MUSS** den Import ablehnen, wenn das über ▸wanPeerRef referenzierte HAN-Kommunikationsprofil nicht im SMGW konfiguriert ist. ▸ [FNN.20014.3] [REQ.FA.CreateProxyConfig.16]
- Das SMGW **SOLL** die Datenfelder gemäß ▸Tabelle 3.46 auf Plausibilität prüfen und im Fehlerfall den Import ablehnen. ▸ [FNN.20014.5] [REQ.FA.CreateProxyConfig.20]
- Das SMGW **MUSS** die Konfigurationsdaten persistieren und für die künftige Proxy-Kommunikation im HAN und WAN verwenden. ▸ [FNN.20014.0] [REQ.FA.CreateProxyConfig.50]

Nr.	Bedingung	Datenfeld	Prüfung
1	▸hanPeerRef HKS gleich TLSPROXY.SOCKS	▸wanPeerRef	Es darf noch kein Proxy-Kommunikationsprofil mit gleicher ▸wanPeerRef Adresse und ▸hanPeerRef konfiguriert sein, da ansonsten eine SOCKS-Signalisierung mit ATYPE=IP4 oder ATYPE=IP6 nicht eindeutig ein Proxy-Profil identifiziert.
2	▸hanPeerRef HKS gleich TLSPROXY.SRV, HKS gleich TLSPROXY.SOCKS	▸localServerName	Es darf noch kein Proxy-Kommunikationsprofil mit gleicher ▸wanPeerRef und ▸hanPeerRef konfiguriert sein, da ansonsten eine TLS-SNI-Signalisierung bzw. SOCKS CONNECT-Signalisierung mit Domain-Name nicht eindeutig ein Proxy-Profil identifiziert.
3	▸hanPeerRef HKS gleich TLSPROXY.CLI	▸wanPeerRef	Es darf noch kein Proxy-Kommunikationsprofil mit gleicher ▸wanPeerRef und ▸hanPeerRef konfiguriert sein, da dies eine redundante Konfiguration darstellt.
4	Immer	▸channelStatus	Das Datenfeld darf nicht vorhanden sein.
5	Das Datenfeld ▸channelPrio ist vorhanden.	▸channelPrio	Es ist noch kein Proxy-Kommunikationsprofil mit gleicher Priorität konfiguriert.

Tabelle 3.46 Plausibilitätsprüfungen

ICS

ICS.FA.CreateProxyConfig.10

Der GWH **MUSS** im ICS deklarieren, welche Plausibilitätsprüfungen gemäß ▸Tabelle 3.46 das SMGW durchführt.

3.15.5 FA.UpdateProxyComProfile

3.15.5.1 Beschreibung

Das SMGW prüft und aktualisiert ein als Aufrufparameter übermitteltes Proxy-Kommunikationsprofil gemäß ▸Proxy-Kommunikationsprofil.

Änderungen sind bis auf folgende Einschränkungen möglich:

- Die Profil-ID und die Referenz auf das HAN-Kommunikationsprofil zum CLS und das WAN-Kommunikationsprofil zum aEMT können nicht geändert werden. In diesen Profilen können die HKS und WKS nicht geändert werden.
- Der localServerName muss im SMGW eindeutig sein.

3.15.5.2 Auslöser

REQ.FA.UpdateProxyConfig.100

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.15.5.3 Anforderungen

- Das SMGW **SOLL** den Import ablehnen, wenn das Profil gemäß ▸Tabelle 3.46 nicht plausibel und eindeutig ist. [REQ.FA.UpdateProxyConfig.10]
- Das SMGW **MUSS** den Import ablehnen, wenn im Profil gemäß ▸Tabelle 3.47 nicht veränderbare Parameter geändert würden ▸ [FNN.20015.4] . [REQ.FA.UpdateProxyConfig.20]
- Das SMGW **MUSS** für fehlende optionale Datenfelder im Aufrufparameter die entsprechenden bereits konfigurierten Daten unverändert lassen. [REQ.FA.UpdateProxyConfig.25]
- Das SMGW **MUSS** die Konfigurationsdaten persistieren und für die künftige Proxy-Kommunikation im HAN und WAN verwenden. ▸ [FNN.20015.0] [REQ.FA.UpdateProxyConfig.30]

Nr.	Bedingung	Datenfeld	Prüfung
1		▸hanPeerRef	Muss identisch mit der bereits im SMGW konfigurierten ▸hanPeerRef sein.
2		▸wanPeerRef	Muss identisch mit der bereits im SMGW konfigurierten ▸wanPeerRef sein.

Tabelle 3.47 Plausibilitätsprüfungen

3.15.6 FA.DeleteProxyComProfile

3.15.6.1 Beschreibung

Das SMGW entfernt ein über den Aufrufparameter identifiziertes, im SMGW konfiguriertes Proxy-Kommunikationsprofil, so dass es nicht mehr für die Proxy-Kommunikation verwendet werden kann.

Noch geöffnete Transportverbindungen zum CLS und aEMT werden zuvor beendet.

Sofern die aus dem Proxy-Kommunikationsprofil referenzierten WAN- und HAN-Kommunikationsprofile nicht mehr referenziert und benötigt werden, können sie anschließend vom GWA gelöscht werden.

3.15.6.2 Auslöser



REQ.FA.DeleteProxyConfig.30

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.15.6.3 Anforderungen

- Das SMGW **MUSS** bestehende, dem ▸wanPeerRef und ▸hanPeerRef zugeordnete TLS-Verbindungen beenden. ▸ [FNN.20016.1] [REQ.FA.DeleteProxyConfig.10]
- Das SMGW **MUSS** das Proxy-Kommunikationsprofil so entfernen, dass damit keine Kommunikationsverbindungen mehr hergestellt werden können. ▸ [FNN.20016.0] [REQ.FA.DeleteProxyConfig.20]

3.15.7 FA.ReadProxyComProfile

3.15.7.1 Beschreibung

Das SMGW exportiert auf Anforderung das im Aufruf identifizierte Proxy-Kommunikationsprofil.

3.15.7.2 Auslöser



REQ.FA.ReadProxyConfig.20

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle SRV.

3.15.7.3 Anforderungen

Das SMGW **MUSS** das über den Aufrufparameter identifizierte Proxy-Kommunikationsprofil gemäß ▸Proxy-Kommunikationsprofil an den Aufrufer exportieren. ▸ [BSI.20031.0] [REQ.FA.ReadProxyConfig.10]

3.16 Monitoring und Diagnose des SMGW (FAKAT.SmgwMonitoring)

3.16.1 Übersicht

Den Anwendungsfällen dieser Kategorie ist gemein, dass der GWA über diese FA den zuverlässigen Betrieb des SMGW gewährleistet. Dazu kann das SMGW Dienste des GWA nutzen (z.B. Firmware-Download oder Zeitsynchronisation) als auch der GWA Dienste des SMGW nutzen (z.B. Abfrage des System-Logs). Die Konfiguration des SMGW zur Erfüllung fachlicher Aufgaben (z.B. Messwertverarbeitung, Proxy-Kommunikation, Wechselprozesse) fällt nicht in diese Kategorie.

3.16.2 Übersicht der FA

Aufgabe	Umsetzung
Ereignis-Protokollierung und Benachrichtigung	
Syslog exportieren	Das SMGW **MUSS** ▸FA.ExportSysLog für den GWA umsetzen. [REQ.WAN.Management.280]
Eichlog exportieren	Das SMGW **MUSS** ▸FA.ExportCalLog für den GWA umsetzen. [REQ.WAN.Management.290]
Löschen der ältesten Eichlog-Einträge	Das SMGW **SOLL** ▸FA.DoTruncateCalLog für den GWA umsetzen. (▸ICS.FAKAT.SmgwMonitoring.20) [REQ.FAKAT.SmgwMonitoring.80]
Übermittlung von Ereignissen und Fehlern an den GWA	Das SMGW **MUSS** ▸FA.DoEventNotification umsetzen. [REQ.WAN.GwaBenachrichtigung.10]
Ereignis protokollieren	Das SMGW **MUSS** ▸FA.EventLog umsetzen. [REQ.WFA.SysLogInhalt.10]
Selbsttest	
Selbsttest auslösen	Das SMGW **MUSS** ▸FA.DoSelftest für den GWA unterstützen. [REQ.WAN.Management.310]
SMGW Zustand	
Vom SMGW für den GWA bereitgestellte Ressourcen (FA und Datenobjekte) ermitteln	Das SMGW **MUSS** ▸FA.ListSmgwResources für den GWA umsetzen. [REQ.FAKAT.SmgwOperation.200]
Software- und Hardwareinformationen des SMGW bereitstellen	Das SMGW **MUSS** ▸FA.ReadDeviceInfo (SMGW-Info) für den GWA umsetzen. [REQ.FAKAT.SmgwMonitoring.10]
Software- und Hardwareinformationen der Messeinrichtung bereitstellen	Das SMGW **MUSS+** ▸FA.ReadDeviceInfo (Meter-Info) für den GWA umsetzen. [REQ.FAKAT.SmgwMonitoring.11]
SMGW Gerätestatus bereitstellen	Das SMGW **SOLL** ▸FA.ReadDeviceStatus des SMGW für den GWA umsetzen. (▸ICS.FAKAT.SmgwMonitoring.20) [REQ.FAKAT.SmgwOperation.170]
WAN-Kommunikationsprofil auslesen	Das SMGW **MUSS** ▸FA.ReadWanComProfile für den GWA umsetzen. [REQ.FAKAT.SmgwOperation.130]
WAN-Schnittstellenkonfiguration auslesen	Das SMGW **MUSS** ▸FA.ReadWanIfProfile für den GWA umsetzen. [REQ.FAKAT.SmgwOperation.140]
HAN-Schnittstellenkonfiguration auslesen	Das SMGW **MUSS** ▸FA.ReadHanIfProfile für den GWA umsetzen. [REQ.FAKAT.SmgwOperation.150]
LMN-Schnittstellenkonfiguration auslesen	Das SMGW **SOLL** ▸FA.ReadLmnIfProfile für den GWA umsetzen. (▸ICS.FAKAT.SmgwMonitoring.20) [REQ.FAKAT.SmgwOperation.160]
Ereignis-Benachrichtigung des GWA ändern	Das SMGW **SOLL** ▸FA.UpdateNotificationProfile für den GWA umsetzen. (▸ICS.FAKAT.SmgwMonitoring.20) [REQ.FAKAT.SmgwMonitoring.50]
Ereignis-Benachrichtigungskonfiguration durch den GWA auslesen	Das SMGW **SOLL** ▸FA.ReadNotificationProfile für den GWA umsetzen. (▸ICS.FAKAT.SmgwMonitoring.20) [REQ.FAKAT.SmgwMonitoring.60]

Aufgabe	Umsetzung
Bereitstellung des Status von Netzwerkschnittstellen zur Diagnose von Verbindungsproblemen	Das SMGW **SOLL** ▸FA.ReadNetworkIfStatus für den GWA umsetzen. (▸ICS.FAKAT.SmgwMonitoring.20) [REQ.FAKAT.SmgwMonitoring.100]

Tabelle 3.48 Übersicht der FA der Kategorie FAKAT.SmgwMonitoring

ICS



ICS.FAKAT.SmgwMonitoring.20

Der GWH **MUSS** im ICS deklarieren, welche MUSS+/SOLL/KANN FAs das SMGW zum Monitoring für den GWA bereitstellt.

3.16.3 Datenstrukturen

Die Datenstruktur für Logbücher ist in ▸Abschnitt 3.22.26 beschrieben.

Die Datenstruktur über Geräteinformationen ist in ▸Abschnitt 3.22.15 beschrieben.

Das Benachrichtigungskonfigurationsprofil ist in ▸Abschnitt 3.22.9 beschrieben.

Die Datenstruktur mit den Selbsttest-Aufrufparametern ist in ▸Abschnitt 3.22.41 beschrieben.

3.16.4 Anforderungen

- Das SMGW **SOLL** den Zeitpunkt des Ausfalls der Versorgungsspannung des SMGW im System-Log protokollieren. ▸ [BSI.6006.0] [REQ.WFA.SysLogInhalt.20]
- Das SMGW **MUSS** nach einem Ausfall der Versorgungsspannung den Zeitpunkt der Wiederkehr der Versorgungsspannung des SMGW im System-Log protokollieren. ▸ [BSI.6001.0] [REQ.WFA.SysLogInhalt.30]
- Das SMGW **MUSS** protokollieren, wenn der verbleibende Speicherplatz für Eichlog-Einträge die Grenze von 10% des für das Eichlog vorgesehenen Speicherplatzes unterschreitet. ▸ [FNN.19008.1] [REQ.FAKAT.SmgwMonitoring.90]

ICS



ICS.WFA.SysLogSpannungsausfall.10

Der GWH **MUSS** im ICS angeben, ob das SMGW den Zeitpunkt des Ausfalls der Versorgungsspannung gemäß ▸REQ.WFA.SysLogInhalt.20 protokolliert.

3.16.5 FA.DoEventNotification

3.16.5.1 Beschreibung

Das SMGW benachrichtigt den GWA über während des Betriebs auftretende Ereignisse oder Fehlersituationen.

3.16.5.2 Auslöser



REQ.FA.NotifySystemEvents.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- WAN-Adresse des SMGW für Wake-Up Dienst hat sich geändert. ▸ [FNN.2008.0]
- Betriebsbereitschaft des SMGW erreicht. ▸ [FNN.17001.0]
- Sofern ein Ereignis ins Syslog protokolliert wird, das gemäß ▸Anhang A unter Berücksichtigung der Konfiguration ▸Abschnitt 3.22.9 zu einer Benachrichtigung des GWA führt.

3.16.5.3 Anforderungen

- Das SMGW **MUSS** die Benachrichtigung des GWA bei Fehlern und Ereignissen über das Kommunikationsszenario ▸WKS.ADMIN-SERVICE durchführen. [REQ.WAN.Kommunikationsszenarien.70]

- Das SMGW **MUSS** mindestens das auslösende Ereignis gemäß ▸Logbuch und Ereignisse an den GWA übermitteln. [REQ.FA.DoEventNotification.10]

3.16.6 FA.ExportSysLog

3.16.6.1 Beschreibung

Das SMGW führt ein System Logbuch (SysLog), in dem betriebsrelevante Ereignisse protokolliert werden.

Das SMGW exportiert die im SysLog gespeicherten Einträge an den Aufrufer. Der Aufrufparameter identifiziert das SMGW.

Über Aufrufparameter kann die exportiere Datenmenge nach Filter-Kriterien begrenzt werden.

3.16.6.2 Auslöser



REQ.FA.ExportSysLog.100

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle SRV.

3.16.6.3 Anforderungen

- Das SMGW **MUSS** über Abfrageparameter den Zeitraum (q.from-q.to) der ausgelesenen Logeinträge eingrenzen können. [REQ.FA.ExportSysLog.10]
- Das SMGW **MUSS** über Abfrageparameter die Anzahl der ausgelesenen Logeinträge begrenzen können. [REQ.FA.ExportSysLog.20]
- Das SMGW **MUSS** unbekannte Abfrageparameter ignorieren. [REQ.FA.ExportSysLog.40]
- Das SMGW **MUSS** die Informationen gemäß ▸Abschnitt 3.22.26 in den Logeinträgen bereitstellen. [REQ.FA.ExportSysLog.50]
- Das SMGW **SOLL** älteste Logeinträge zuerst übertragen, sofern ein Abfrageparameter nicht etwas anderes festlegt. [REQ.FA.ExportSysLog.60]
- Das SMGW **SOLL** die exportierten Logeinträge über einen Abfrageparameter auf einen "Level" (I, W, E, F) einschränken können. [REQ.FA.ExportSysLog.70]
- Sofern der Aufrufparameter "q.signed=CMS_ECDSA_SHA256_Detached" einen signierten Export des Logs anfordert, **SOLL** das SMGW die Export-Signatur ▸signature.sigValue über die kanonisierten Datenfelder der Export-Struktur mit dem Algorithmus CMS_ECDSA_SHA256_Detached und dem Signaturschlüssel des SMGW (GW_WAN_SIG_PRV) berechnen. Das Datenfeld sigValue selbst geht nicht in die Signaturberechnung ein. [REQ.FA.ExportSysLog.80]
- Das SMGW **MUSS** das SysLog gemäß ▸Tabelle 3.49 in der Export-Struktur ▸Abschnitt 3.22.17 an den Aufrufer übermitteln. [REQ.FA.ExportSysLog.90]

Export Datenfeld	Ursprung
▸exportedData	Siehe ▸Tabelle 3.87
▸tafId	Entfällt
▸tafId.mpId	Entfällt
▸tafId.meteringPointId	Entfällt
▸gatewayId	Herstellerübergreifende Identifikationsnummer des exportierenden SMGW (entspricht der SubjectCN in GW_WAN_TLS_CRT, GW_WAN_SIG_CRT und GW_WAN_ENC_CRT)
▸signature	Entfällt, sofern gemäß Query-Parameter "q.signed" keine Signatur erstellt wird.
▸signature.algo	Gemäß in Query-Parameter "q.signed" verwendetem Algorithmus
▸signature.ts	Systemzeit des SMGW beim Aufruf (Signaturerstellungszeitpunkt)

Export Datenfeld	Ursprung
▸signature.originator	Die herstellerübergreifend eindeutige Identifikation des SMGW (Siehe ▸Abschnitt 5.3)
▸signature.sigValue	Codierung und Wert gemäß in Query-Parameter "q.signed" verwendetem Verfahren

Tabelle 3.49 Übernahme von Datenfeldern in die Exportstruktur eines Logbuchs

ICS



ICS.FA.ExportSysLog.10

Der GWH **MUSS** im ICS deklarieren, welche Filterparameter zur Begrenzung der exportieren Logeinträge ausgewertet werden.



ICS.FA.ExportSysLog.80

Der GWH **MUSS** im ICS deklarieren, ob die Export-Signatur ▸signature.sigValue über die kanonisierten Datenfelder der Export-Struktur mit dem Algorithmus CMS_ECDSA_SHA256_Detached und dem Signaturschlüssel des SMGW (GW_WAN_SIG_PRV) berechnet wird, sofern der Aufrufparameter "q.signed=CMS_ECDSA_SHA256_Detached" einen signierten Export des Logs anfordert.

3.16.7 FA.ExportCalLog

3.16.7.1 Beschreibung

Dem SMGW führt ein Eichlog, in dem Ereignisse für Aufgaben gemäß [MessEG]/[MessEV] protokolliert werden.

Das SMGW exportiert die im Eichlog gespeicherten Einträge an den Aufrufer. Der Aufrufparameter identifiziert das SMGW.

Die Anfrage kann Abfrageparameter enthalten, die die Menge der exportierten Logbucheinträge nach Ereignistyp oder Zeitraum begrenzt.

3.16.7.2 Auslöser



REQ.FA.ExportCalLog.100

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle SRV.

3.16.7.3 Anforderungen

- Das SMGW **MUSS** über Abfrageparameter den Zeitraum (Von-Bis) der ausgelesenen Logeinträge eingrenzen können. [REQ.FA.ExportCalLog.10]
- Das SMGW **MUSS** über Abfrageparameter die Anzahl der ausgelesenen Logeinträge begrenzen können. [REQ.FA.ExportCalLog.20]
- Das SMGW **SOLL** die exportierten Logeinträge über einen Abfrageparameter auf eine Ereignis-ID eingrenzen können. [REQ.FA.ExportCalLog.30]
- Das SMGW **MUSS** unbekannte Abfrageparameter ignorieren. [REQ.FA.ExportCalLog.40]
- Das SMGW **MUSS** die Informationen gemäß ▸Abschnitt 3.22.26 in den Logeinträgen bereitstellen. [REQ.FA.ExportCalLog.50]
- Das SMGW **SOLL** älteste Logeinträge zuerst übertragen, sofern ein Abfrageparameter nicht etwas anderes festlegt. [REQ.FA.ExportCalLog.60]
- Das SMGW **SOLL** die exportierten Logeinträge über einen Abfrageparameter auf einen "Level" (I, W, E, F) einschränken können. [REQ.FA.ExportCalLog.70]

- Sofern der Abfrageparameter "q.signed=CMS_ECDSA_SHA256_Detached" einen signierten Export des Logs anfordert, **MUSS** das SMGW die Export-Signatur ▸signature.sigValue über die kanonisierten Datenfelder der Export-Struktur mit dem Algorithmus CMS_ECDSA_SHA256_Detached, dem Signaturschlüssel des SMGW (GW_WAN_SIG_PRV) berechnen. Das Datenfeld "sigValue" selbst geht nicht in die Signaturberechnung ein. [REQ.FA.ExportCalLog.80]
- Das SMGW **MUSS** das Eichlog gemäß ▸Tabelle 3.49 in der Export-Struktur ▸Exportstruktur an den Aufrufer übermitteln. ▸ [BSI.20036.0] [REQ.FA.ExportCalLog.90]

ICS



ICS.FA.ExportCalLog.10

Der GWH **MUSS** im ICS deklarieren, welche Filterparameter zur Begrenzung der exportieren Logeinträge ausgewertet werden.



ICS.FA.ExportCalLog.20

Der GWH **MUSS** im ICS deklarieren, ob älteste Logeinträge zuerst übertragen werden, wenn ein Aufrufparameter nichts anders bestimmt.



ICS.FA.ExportCalLog.30

Der GWH **MUSS** im ICS deklarieren, ob die exportierten Logeinträge über einen Abfrageparameter auf eine Ereignis-ID eingegrenzt werden können.

3.16.8 FA.ReadNetworkIfStatus

3.16.8.1 Beschreibung

Das SMGW stellt dem Aufrufer Informationen zu Status und Betriebsart der im Aufrufparameter benannten physischen Netzwerkschnittstelle des SMGW bereit. Die zulässigen Datenfelder sind in ▸Abschnitt 3.22.31 aufgelistet.

3.16.8.2 Auslöser



REQ.FA.ReadNetworkIfStatus.30

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle SRV.

3.16.8.3 Anforderungen

- Das SMGW **MUSS** dem Aufrufer die Schnittstelleninformationen bereitstellen. [REQ.FA.ReadNetworkIfStatus.10]
- Das SMGW **MUSS** die exportierten Netzwerk-Statusinformationen gemäß der in ▸ICS.HAN.ServiceTechnikerDatenbereitstellung.10 beschriebenen Query-Parameter begrenzen. [REQ.FA.ReadNetworkIfStatus.20]

ICS



ICS.HAN.ServiceTechnikerDatenbereitstellung.10

Der GWH **MUSS** im ICS für die vom SMGW verarbeiteten Query Parameter die Bezeichner, Bedeutung und Wertebereiche beschreiben (Liste "attribut": Bedeutung).

3.16.9 FA.ReadWanIfProfile

3.16.9.1 Beschreibung

Die Konfigurationsparameter der im Aufrufparameter identifizierten WAN-Netzwerk-Zugangsschnittelle werden exportiert.

3.16.9.2 Auslöser



REQ.FA.ReadWanIfProfile.20

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle SRV.

3.16.9.3 Anforderungen

Das SMGW **MUSS** die Konfiguration des über den Aufrufparameter identifizierten WAN-Schnittstellenkonfigurationsprofils gemäß ▸WAN-Schnittstellenkonfigurationsprofil an den Aufrufer exportieren. [REQ.FA.ReadWanIfProfile.10]

3.16.10 FA.ReadHanIfProfile

3.16.10.1 Beschreibung

Die Konfigurationsparameter einer HAN-Netzwerkschnittstelle werden exportiert.

3.16.10.2 Auslöser



REQ.FA.ReadHanIfProfile.20

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle SRV.

3.16.10.3 Anforderungen

Das SMGW **MUSS** das über den Aufrufparameter identifizierte ▸HAN-Schnittstellenkonfigurationsprofil an den Aufrufer exportieren. [REQ.FA.ReadHanIfProfile.10]

3.16.11 FA.ReadLmnIfProfile

3.16.11.1 Beschreibung

Die Konfigurationsparameter der LMN-Netzwerkschnittelle werden exportiert.

3.16.11.2 Auslöser



REQ.FA.ReadLmnIfProfile.20

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle SRV.

3.16.11.3 Anforderungen

Das SMGW **MUSS** die Konfiguration des über den Aufrufparameter identifizierten LMN-Schnittstellenkonfigurationsprofils gemäß ▸Abschnitt 3.22.24 an den Aufrufer exportieren. [REQ.FA.ReadLmnIfProfile.10]

3.16.12 FA.EventLog

3.16.12.1 Beschreibung

Protokolliert ein im SMGW aufgetretenes Ereignis.

Es sind mindestens die folgenden drei Klassen von Logbüchern zu implementieren. ▸Tabelle 3.50 bietet eine Übersicht über die verschiedenen Logbücher und die zulässigen Zugriffe.

Log-Klasse	Beschreibung	Zugriff	Schnittstelle
System-Log	Das System-Log dient der Bereitstellung von betriebsrelevanten Ereignissen für den GWA bzw. Betreiber des SMGW, sodass dieser die Möglichkeit erhält Störungen, Fehler und weitere Ereignisse im Betrieb nachzuvollziehen. Das Logbuch ist als Ringspeicher ausgeführt.	Lesender Zugriff durch den autorisierten GWA.	WAN-Schnittstelle
		Lesender Zugriff durch den autorisierten Servicetechniker (SRV).	HAN-Schnittstelle
Anschlussnutzer-Log	Das Anschlussnutzer-Log dient der Bereitstellung von abrechnungsrelevanten Daten und Tarifinformationen für den Anschlussnutzer, so dass dieser die Möglichkeit erhält nachzuvollziehen, welche Messwerte für die Abrechnung verwendet wurden. Des Weiteren gibt es dem Anschlussnutzer die Möglichkeit zu erfahren, welche Daten an EMT versendet wurden. Das Logbuch ist als Ringspeicher ausgeführt.	Lesender Zugriff nur durch den authentifizierten und autorisierten Anschlussnutzer (CON) auf die ihm zugeordneten Log-Einträge.	HAN-Schnittstelle
Eichtechnisches Log	Das Eichtechnische Log dient der Registrierung von Änderungen an eichtechnisch relevanten Soft- und Firmwareanteilen sowie den Konfigurationsprofilen und den zugehörigen Parametern. Des Weiteren müssen im Eichtechnischen Log nach [MessEG]/[MessEV] relevante Ereignisse gespeichert werden, so dass nachträglich erkennbar ist, ob und welche Messwerte verfälscht worden sind. Das Logbuch kann als Ringspeicher ausgeführt werden.	Lesender Zugriff durch den autorisierten GWA.	WAN-Schnittstelle

Tabelle 3.50 Logbuch-Klassen und erlaubter Zugriff

3.16.12.2 Auslöser

REQ.FA.EventLog.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Ereignis gemäß ▸Anhang A tritt auf.
- IT-sicherheitsbezogenes Audit-Ereignis gemäß ▸Abschnitt 5.7 tritt auf.

3.16.12.3 Anforderungen

- Das SMGW **SOLL** im Syslog-Ringspeicher mindestens 10000 Einträge speichern können. [REQ.WFA.Logformat.40]
- Zur Vermeidung einer zu schnellen Verdrängung von Ereignissen aus einem Ringspeicher-Logbuch **SOLL** das SMGW innerhalb eines Zeitraumes aufeinanderfolgende Ereignisse mit gleicher Ereignis-Identifikation zusammenfassend speichern. Insbesondere gilt dies für Fehler, die vor oder bei dem Herstellen einer authentisierten Verbindung auftreten. ▸ICS.FA.EventLog.20 [REQ.WFA.Logformat.50]
- Das SMGW **SOLL** die Einträge im Anschlussnutzer-Log löschen, die älter als ▸maxLogDuration sind. (▸ICS.FA.EventLog.30 [REQ.FA.EventLog.20]

ICS

ICS.FA.EventLog.10

Der GWH **MUSS** im ICS angeben, wie viele Syslog-Einträge das SMGW mindestens persistieren kann.

ICS.FA.EventLog.20

Der GWH **MUSS** im ICS angeben (in Sekunden), über welchen Zeitraum identische Logeinträge (Syslog, Userlog, Eichlog) gesammelt und zusammengefasst werden.



ICS.FA.EventLog.30

Der GWH **MUSS** im ICS deklarieren, welche maximale Vorhaltefrist (in Tagen) für das Anschlussnutzer-Log gilt, wenn der Parameter ▸maxLogDuration nicht konfiguriert ist.



ICS.FA.EventLog.40

Der GWH **MUSS** im ICS deklarieren in welchem Bereich die Vorhaltefrist (maxLogDuration) für das Anschlussnutzer-Log konfiguriert werden kann.

3.16.13 FA.DoSelftest

3.16.13.1 Beschreibung

Das SMGW führt über Parameter näher bestimmte Selbsttest/Audit-Log-Funktionen gemäß [CC] und [MessEG]/[MessEV] im SMGW aus, deren Ergebnis im Syslog bzw. Eichlog protokolliert wird. Ohne nähere Bestimmung des Selbsttests über einen Aufrufparameter (▸Abschnitt 3.22.41 wird durch diesen FA die Integrität und Authentizität der Firmware, Konfigurationsdaten und der Nutzerdaten wie beispielsweise der abrechnungsrelevanten persistierten Messwerte geprüft und das Ergebnis protokolliert.

Ein Integritätsfehler (Details siehe ▸Abschnitt 3.16.13.3) wird als "Fataler Fehler des SMGW" gewertet und im kombinierten Statuswort für die künftige Registrierung von Messwerten in ▸Abschnitt 3.22.13 vermerkt.

3.16.13.2 Auslöser



REQ.FA.DoSelftest.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle SRV.
- Automatisch nach dem Neustart des SMGW.
- Regelmäßig selbstständig gemäß ▸ICS.FA.DoSelftest.10.

▸ [BSI.15002.0]

3.16.13.3 Anforderungen

- Das SMGW **MUSS** die Integrität und Authentizität der Firmware/Software vor absichtlicher Veränderung prüfen, indem die Signatur validiert wird. Validierungsfehler sind "Fatale" Fehler. ▸ [BSI.15001.0] ▸ [BSI.15001.1] [REQ.WAN.Selbsttest.10]
- Das SMGW **MUSS** die Integrität der Auswertungsprofile, Zeitsynchronisations- und Kommunikationsprofile und des persistenten kryptografischen Materials (Schlüssel und Zertifikate) vor zufälligen und unbeabsichtigten Veränderungen prüfen, indem eine Prüfsumme oder ein kryptografischer Hash über diese Daten berechnet wird, der mit dem Vergleichswert unmittelbar nach der letzten durch das SMGW autorisierten Veränderung verglichen wird. Validierungsfehler sind "Fatale" Fehler. ▸ [BSI.15001.1] [REQ.WAN.Selbsttest.20]
- Das SMGW **MUSS** die Integrität der persistierten Wertelisten (AWL, RWL, TWL), des Eichlogs und der Anschlussnutzer-Logs vor zufälligen und unbeabsichtigten Veränderungen prüfen, indem eine Prüfsumme oder ein kryptografischer Hash über diese Daten berechnet wird, der mit dem Vergleichswert unmittelbar nach der letzten durch das SMGW autorisierten Veränderung verglichen wird. Validierungsfehler sind "Fatale" Fehler. ▸ [BSI.15001.1] [REQ.WAN.Selbsttest.21]
- Das SMGW **MUSS** im kombinierten Statuswort (▸Kombiniertes Statuswort) bei einem Signatur-Validierung-Fehler der Firmware oder einem festgestellten Integritätsfehler der Auswertungs-, Zeitsynchronisations- oder Kommunikationsprofile oder der persistierten Wertelisten ▸smgwStatus.error gleich "true" (SMGW_Error) setzen. [REQ.WAN.Selbsttest.70]
- Das SMGW **MUSS** im kombinierten Statuswort (▸Kombiniertes Statuswort) ▸smgwStatus.error gleich "true" (SMGW_Error) setzen, wenn das Sicherheitsmodul nicht erreichbar ist oder einen Selbsttestfehler meldet. [REQ.WAN.Selbsttest.80]

ICS



ICS.FA.DoSelftest.10

Der GWH **MUSS** im ICS (in Sekunden) angegeben, in welchem Zeitabstand (maximal) der regelmäßige, automatische Selbsttest vom SMGW ausgelöst wird.

3.16.13.4 Implementierungshinweise

Für die Integritätssicherung von Firmware- und Konfigurationsdaten (Parameter) wird eine kryptografische Prüfsumme, mindestens SHA-256 empfohlen.

Gemäß [PP-0073] führt der Selbsttest zu Audit-Log-Einträgen (siehe ▸Abschnitt 5.7).

3.16.14 FA.ListSmgwResources

3.16.14.1 Beschreibung

Das SMGW exportiert die Identifikation aller zugeordneten FA oder Ressourcen (Datenobjekte), die das SMGW für den authentifizierten und berechtigten Nutzer bereitstellt.

Aufrufparameter begrenzen die Auswahl nach zugeordneten FA oder Typ der Ressource.

Je nach Typ der Ressource kann ein Aufrufer auf dieser Ressource Operationen ausführen (z.B. Lesen, Aktualisieren, Anlegen, Löschen, Aufrufen)

3.16.14.2 Auslöser



REQ.FA.ListSmgwResources.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Empfang einer Anfrage über ▸HKS.WS1.
- Empfang einer Anfrage über ▸HKS.WS2.

3.16.14.3 Anforderungen

Das SMGW **MUSS** die zugeordneten FA oder Ressourcen gemäß [DS] Kapitel "RESTful Webservice Protokoll", Abschnitt "URI-Pfade" auflisten. [REQ.FA.ListSmgwResources.20]

3.16.15 FA.ReadDeviceInfo

3.16.15.1 Beschreibung

Stellt für das über den Aufrufparameter (Ressource-ID) identifizierte Gerät Hardware-Typ, Software/Firmware-Identifikation und Version bereit. [12] Die Identifikation der Firmware/Software wird vom Hersteller des Gerätes vergeben und identifiziert diese eindeutig. Diese Informationen können im Rahmen von Konformitätsbewertungsverfahren referenziert werden.

Die ▸deviceId entspricht der Kennzeichnung des Gerätes auf dem Gehäuse (Für das SMGW siehe ▸Abschnitt 5.3). Wird als Geräte-Identifikation die Identifikation einer über ein LMN-Kommunikationsprofil an das SMGW kommunikativ angebundenen Messeinrichtung übergeben, hängt die Übermittlung der Messgeräteinformation von den Fähigkeiten der Messeinrichtung ab (siehe ▸FA.RetrieveDeviceInfoFromMtr).

3.16.15.2 Auslöser



REQ.FA.ReadDeviceInfo.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT von der Rolle GWA.

[12] Sofern mehrere Software-Teile identifizierbar sind, sind mindestens die Teile der Software, die nach [MessEG] und [MsbG] relevant sind eindeutig über eine (kryptografische) Prüfsumme zu identifizieren.

- Empfang einer Anfrage über ▸HKS.WS1 von der Rolle CON.
- Empfang einer Anfrage über ▸HKS.WS1 von der Rolle CLS.
- Empfang einer Anfrage über ▸HKS.WS1 von der Rolle SRV.
- Empfang einer Anfrage über ▸HKS.WS2 von der Rolle CON.

3.16.15.3 Anforderungen

- Sofern die Geräte-ID im Aufrufparameter einer ▸meterId eines LMN-Kommunikationsprofils entspricht **MUSS+** das SMGW die über ▸FA.RetrieveDeviceInfoFromMtr erhaltenen Informationen (installierte Software-Version, Hardware-Typ) an den Aufrufer bereitstellen. [REQ.FA.ReadDeviceInfo.20]
- Sofern die Geräte-ID im Aufrufparameter das SMGW identifiziert, **MUSS** das SMGW mindestens die Datenfelder ▸swVersions an den Aufrufer übermitteln. [REQ.FA.ReadDeviceInfo.30]
- Das SMGW **MUSS** die Geräte-Informationen des über den Aufrufparameter identifizierten Gerätes mittels ▸Device-Info über das aufrufende Kommunikationsszenario an den Aufrufer bereitstellen. [REQ.FA.ReadDeviceInfo.40]

3.16.16 FA.ReadDeviceStatus

3.16.16.1 Beschreibung

Stellt für das über den Aufrufparameter (Ressource-ID) identifizierte Gerät das Geräte-Statuswort gemäß [DS] Kapitel "Messwertstatus" bereit. Das Statuswort gibt Auskunft über Fehler, Warnungen und Zustände des Gerätes.

Da das Statuswort keine Informationen zum Verbrauch enthält, ist die Abfrage des Messgerätestatuswortes nicht an eine Berechtigung über ein Auswertungsprofil gebunden.

3.16.16.2 Auslöser



REQ.FA.ReadDeviceStatus.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT
- Empfang einer Anfrage über ▸HKS.WS1 für die Rolle CON, SRV
- Empfang einer Anfrage über ▸HKS.WS2 für die Rolle CON

3.16.16.3 Anforderungen

- (▸role ungleich "SRV") Das SMGW **MUSS** die Anfrage ablehnen, wenn der Aufrufparameter einer ▸meterId eines LMN-Kommunikationsprofils entspricht. [REQ.FA.ReadDeviceStatus.15]
- Sofern die Geräte-ID im Aufrufparameter einer ▸meterId eines LMN-Kommunikationsprofils entspricht **MUSS** das SMGW das zuletzt von der Messeinrichtung erhaltene Statuswort gemäß [DS] Kapitel Messwertstatus übermitteln. [REQ.FA.ReadDeviceStatus.20]
- Sofern die Geräte-ID im Aufrufparameter das SMGW identifiziert, **MUSS** das SMGW das aktuelle SMGW-Statuswort gemäß [DS] Kapitel Messwertstatus übermitteln. [REQ.FA.ReadDeviceStatus.30]
- Das SMGW **MUSS** das Geräte-Statuswort mittels ▸Device-Status über das aufrufende Kommunikationsszenario an den Aufrufer bereitstellen. [REQ.FA.ReadDeviceStatus.40]

3.16.17 FA.UpdateNotificationProfile

3.16.17.1 Beschreibung

Das SMGW benachrichtigt den GWA gemäß ▸Anhang A über relevante Ereignisse.

Damit der GWA seine Kommunikationssysteme vor massenhaften Benachrichtigungen schützen kann oder in individuellen Situationen bei Eintreten von Ereignissen benachrichtigt wird, gibt dieser FA dem Aufrufer die Möglichkeit, die Voreinstellungen für die Benachrichtigung des GWA (defaults) zu verändern.

Der Aufrufparameter enthält das gesamte ▸Benachrichtigungsprofil für alle Ereignisse.

Der Aufruf wird (ohne Veränderung der Konfiguration) abgelehnt, wenn die Liste ungültige Einträge enthält. Ungültig sind beispielsweise nicht eindeutige Ereignistypen.

3.16.17.2 Auslöser



REQ.FA.UpdateNotificationProfile.30

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.16.17.3 Anforderungen

- Das SMGW **MUSS** die Aktualisierung ablehnen, sofern das Tupel der Datenfeldinhalte aus ▸notificationEvents ("vendor", "eventId", "eventSubId") mehrfach in der Ereignis-Liste des Aufrufparameters vorhanden ist. [REQ.FA.UpdateNotificationProfile.10]
- Das SMGW **MUSS** die als Aufrufparameter übergebene ▸Benachrichtigungsprofil persistieren und künftig für die Ereignis-Benachrichtigung des GWA (siehe ▸FA.DoEventNotification) verwenden. [REQ.FA.UpdateNotificationProfile.20]

3.16.18 FA.ReadNotificationProfile

3.16.18.1 Beschreibung

Dieser FA exportiert die Liste der Ereignisse (▸Abschnitt 3.22.9), über die der GWA benachrichtigt wird an den Aufrufer.

Ist nach der Inbetriebnahme keine Veränderung des Benachrichtigungsprofiles erfolgt, entspricht die Liste den Standardwerten zur GWA-Benachrichtigung gemäß ▸Anhang A.

3.16.18.2 Auslöser



REQ.FA.ReadNotificationProfile.20

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.16.18.3 Anforderungen

Das SMGW **MUSS** die Ereignisse, über die der GWA benachrichtigt wird gemäß ▸Benachrichtigungsprofil über das auslösende Kommunikationsszenario an den Aufrufer übermitteln. [REQ.FA.ReadNotificationProfile.10]

3.16.19 FA.DoTruncateCalLog

3.16.19.1 Beschreibung

Das SMGW entfernt die ältesten Eichlog-Einträge, die vor einem als Aufrufparameter (siehe ▸Parameter zum Verkürzen von Logs) übergebenen Datum liegen.

Der GWA gewährleistet vor dem Aufruf dieses FA, dass die für künftige Nachweise notwendigen Eichlog-Einträge exportiert und archiviert wurden.

Das SMGW protokolliert im Eichlog die Identifikation des auslösenden GWA und Informationen zum Nachweis der Vollständigkeit der beim GWA archivierten Eichlog-Einträge.

Der GWA gewährleistet die Einhaltung der Vorhaltefristen ▸Tabelle 5.1 durch Archivierung exportierter Eichlog-Einträge.



Warnung

Werden im Rahmen dieses FA Logeinträge gelöscht, ist zu beachten, dass die eichrechtlichen Fristen durch geeignete Aufbewahrung in signierter Form außerhalb des SMGW sichergestellt werden

müssen. Ein Export kann durch den GWA oder den Servicetechniker mittels ▸FA.ExportCalLog in signierter Form erfolgen.

3.16.19.2 Auslöser



REQ.FA.DoTruncateCalLog.50

Das SMGW**MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle SRV.

3.16.19.3 Anforderungen

- Das SMGW **MUSS** einen Aufruf ohne Aufrufparameter oder mit einem in der Zukunft liegenden Aufrufparameter ▸truncationDateTime ablehnen. [REQ.FA.DoTruncateCalLog.10]
- Das SMGW **MUSS** im Eichlog protokollieren, wie viele Eichlog-Einträge gelöscht wurden, die fortlaufende Nummer des ältesten und jüngsten gelöschten Eintrages und die Identität des Aufrufers des FA (GWA-ID aus dem SubjectCN). Dabei wird der ▸idx lückenlos nach dem bisher höchsten (jüngsten) Index fortgesetzt. ▸ [PTB.19012.0] [REQ.FA.DoTruncateCalLog.20]
- Das SMGW **MUSS** die Eichlog-Einträge, die zeitlich vor dem als Aufrufparameter ▸truncationDateTime übergebenen Zeitpunkt liegen so löschen, dass sie nicht mehr ausgelesen werden können und dabei die Integrität der nicht gelöschten Einträge gewährleisten. [REQ.FA.DoTruncateCalLog.30]
- Das SMGW **MUSS** die folgenden Eichlog-Einträge weiterhin im Eichlog aufbewahren: erkannte Integritätsfehler (▸ [BSI.19001.1]), erfolgreiche Firmware-Updates (▸ [BSI.18009.0]), dauerhafte Störung der Sicherheitsfunktionalität (▸ [BSI.4010.2]). [REQ.FA.DoTruncateCalLog.40]

3.17 Administrationsvoraussetzungen herstellen und erhalten (FAKAT.SmgwAdministration)

3.17.1 Übersicht

Die Anwendungsfälle dieser Kategorie beschreiben die Funktionalität des SMGW zur sicheren und interoperablen kommunikativen Anbindung des GWA und die damit verbundenen Voraussetzungen zur Herstellung und Wahrung eines administrativen Zugriffs.

Die FA sind so beschrieben, dass durch das Verhalten des SMGW eine Ausfallsicherheit beim Zertifikatswechsel von GWA-Zertifikaten gegeben ist. Das setzt Prozesse beim GWA voraus, die diese Ablaufreihenfolge (erst Importieren/Erzeugen von Zertifikaten und Schlüsseln, dann Deaktivieren von Zertifikaten und Schlüsseln) unterstützen.

In diesem Kapitel werden Zertifikats-Datenobjekte im Rahmen von Wechsel- oder Aktualisierungsprozessen mit einem Suffix n gekennzeichnet, welches die zeitliche Abfolge der Verwendung des Zertifikates ordnet. Dabei bezeichnet n-1 ein künftig nicht mehr zu verwendendes Zertifikat und n+1 das künftige Zertifikat.

Wechselprozesse zwischen verschiedenen GWA werden in [TR-03109-1-VI] beschrieben.

▸Tabelle 3.51 listet die vom SMGW zu unterstützenden FAs für die Herstellung der Administrationsvoraussetzungen auf.

Initiale GWA-WAN-Kommunikationsprofile für den operativen (Ressourcen-Zugriffs-Domäne "GWA") und den künftigen GWA (Ressourcen-Zugriffs-Domäne "GWAPRE") werden im Rahmen der Vorpersonalisierung/Initialkonfiguration bzw. bei der Konvertierung der WAN-Kommunikationsprofile aus der vorherigen Firmwareversion erzeugt. Der Inhalt der GWA-WAN-Kommunikationsprofile wird vom Besteller festgelegt und vom GWH konfiguriert. Die GWA-WAN-Kommunikationsprofile können im Wirkbetrieb weder erzeugt, noch gelöscht werden. Sie können aktualisiert und gelesen werden.

3.17.2 Übersicht der FA

Aufgabe	Umsetzung
Anfordern einer Kommunikationsverbindung zur Administration des SMGW	Das SMGW **MUSS** ▸FA.InitiateManagementConnection für den GWA umsetzen. [REQ.WAN.WakeUp.10]
GWA-Zertifikate im SMGW aktualisieren	Das SMGW **MUSS** ▸FA.DoImportGwaKeys für den GWA umsetzen. [REQ.WAN.Management.190] Die Aktualisierung erfolgt über ▸FA.UpdateWanComProfile.
GWA-Zertifikate im SMGW deaktivieren	Das SMGW **MUSS** ▸FA.DoDeactivateGwaCerts für den GWA umsetzen. [REQ.WAN.Management.195]
GWA-Kommunikationsprofil aktualisieren	Das SMGW **MUSS** ▸FA.UpdateWanComProfile für den GWA (Ressource-Domäne "gwa" und "gwapre") umsetzen. [REQ.FAKAT.SmgwAdministration.10]
Parameter der physischen WAN-Schnittstelle ändern	Das SMGW **SOLL** ▸FA.UpdateWanIfProfile für den GWA umsetzen. (siehe ▸ICS.FAKAT.SmgwAdministration.10) [REQ.WAN.Management.260]
Parameter der physischen HAN-Schnittstelle ändern	Das SMGW **SOLL** ▸FA.UpdateHanIfProfile für den GWA umsetzen. (siehe ▸ICS.FAKAT.SmgwAdministration.10) [REQ.FAKAT.SmgwAdministration.90]
Parameter der physischen LMN-Schnittstelle ändern	Das SMGW **SOLL** ▸FA.UpdateLmnIfProfile für den GWA umsetzen. (▸ICS.FAKAT.SmgwAdministration.10) [REQ.FAKAT.SmgwAdministration.100]
Challenge zur Authentifizierung des GWA am Sicherheitsmodul anfordern	Das SMGW **MUSS** ▸FA.DoRequestSecmodAuth für den GWA umsetzen. [REQ.WAN.Management.162]
Authentifizierung des GWA am Sicherheitsmodul	Das SMGW **MUSS** ▸FA.DoResponseSecmodAuth für den GWA umsetzen. [REQ.WAN.Management.160]
Authentifizierung des GWA am Sicherheitsmodul beenden	Das SMGW **MUSS** ▸FA.DoFinishSecmodAuth für den GWA umsetzen. [REQ.WAN.Management.161]
Nutzerdatenbereinigung durch GWA	Das SMGW **MUSS+** ▸FA.DoDeleteUserData für den GWA umsetzen. (▸ICS.FAKAT.SmgwAdministration.10) [REQ.FAKAT.SmgwAdministration.70]
Neustart des SMGW	Das SMGW **MUSS** ▸FA.DoReboot für den GWA umsetzen. [REQ.FAKAT.SmgwAdministration.80]

Tabelle 3.51 Übersicht der FA der Kategorie FAKAT.SmgwAdministration

ICS



ICS.FAKAT.SmgwAdministration.10

Der GWH **MUSS** im ICS deklarieren, welche FAs das SMGW für den GWA unterstützt.

3.17.3 Datenstrukturen der FA-Kategorie

Das GWA-WAN-Kommunikationsprofil ist in ▸Abschnitt 3.22.46 beschrieben.

Das WAN-Schnittstellenkonfigurationsprofil ist in ▸Abschnitt 3.22.45 beschrieben.

Das HAN-Schnittstellenkonfigurationsprofil ist in ▸Abschnitt 3.22.21 beschrieben.

Das LMN-Schnittstellenkonfigurationsprofil ist in ▸Abschnitt 3.22.24 beschrieben.

Die Datenstruktur mit den GWA-Importzertifikaten ist in ▸Abschnitt 3.22.20 beschrieben.

Die Datenstruktur mit den Auth-Challenge-Parametern ist in ▸Abschnitt 3.22.7 beschrieben.

Die Datenstruktur mit den Auth-Response-Parametern ist in ▸Abschnitt 3.22.8 beschrieben.

3.17.4 FA.CreateWanComProfile

3.17.4.1 Beschreibung

Das SMGW prüft und persistiert das als Aufrufparameter übergebene WAN-Kommunikationsprofil für die kommunikative Anbindung eines EMT. Das WAN-Kommunikationsprofil wird verwendet, um damit die initiale kommunikative Anbindung eines EMT für den Messwertversand zu konfigurieren.

Nachdem das SMGW die Plausibilität der Aufrufparameter (▸Abschnitt 3.22.46) überprüft hat, wird das WAN-Kommunikationsprofil importiert, persistiert und die Kommunikationsparameter für die Kommunikation mit dem EMT verwendet.

Über diesen FA werden neue WAN-Kommunikationsprofile für einen EMT konfiguriert. Zulässige WKS sind ▸WKS.INFO-REPORT, ▸WKS.TLSPROXY im SMGW konfiguriert.

Nach dem Aufruf des FA für ein EMT-WAN-Kommunikationsprofil werden die EMT-Kommunikationsparameter unmittelbar verwendet.

3.17.4.2 Auslöser



REQ.FA.CreateWanComProfile.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.17.4.3 Anforderungen

- Das SMGW **SOLL** die Datenfelder gemäß ▸Tabelle 3.52 auf Plausibilität prüfen und im Fehlerfall den Import ablehnen. ▸ [FNN.20001.2] [REQ.FA.CreateWanComProfile.20]
- Das SMGW **MUSS** den Import ablehnen, wenn bereits ein WAN-Kommunikationsprofil mit identischer ▸profileId konfiguriert ist. ▸ [FNN.20001.3] [REQ.FA.CreateWanComProfile.50]
- Das SMGW **MUSS** das WAN-Kommunikationsprofil persistieren und die Parameter und die enthaltenen Zertifikate künftig für die Kommunikation mit dem Kommunikationspartner verwenden. ▸ [FNN.20001.0] [REQ.FA.CreateWanComProfile.30]

▸Tabelle 3.52 beschreibt Plausibilitätsprüfungen beim Import von WAN-Kommunikationsprofilen.

Nr.	Bedingung	Datenfeld	Prüfung
1	Immer	▸peerCerts.tlsCert, ▸peerCerts.sigCert, ▸peerCerts.encCert	Alle Datenfelder sind vorhanden und DER-Codiert gemäß [X.690].
2	▸wks ist gleich ▸WKS.MANAGEMENT, ▸WKS.ADMIN-SERVICE, ▸WKS.NTP-TLS, ▸WKS.DOWNLOAD	▸peerCerts.tlsCert, ▸peerCerts.sigCert, ▸peerCerts.encCert	Alle *SubjectCN* entsprechen [SM-PKI-CP] Anhang A (SM-PKI) oder C (SM-Test-PKI) für die Funktion "gwa".
3	▸wks ist gleich ▸WKS.INFO-REPORT	▸peerCerts.encCert	Der *SubjectCN* entspricht [SM-PKI-CP] Anhang A (SM-PKI) oder C (SM-Test-PKI) für die Funktion "emt".
4	▸wks ist gleich ▸WKS.MANAGEMENT, ▸WKS.ADMIN-SERVICE.	▸peerCerts.tlsCert, ▸peerCerts.sigCert, ▸peerCerts.encCert	Der SubjectDN der SIG/ENC/TLS-Zertifikate stimmt überein.
5	▸wks ist gleich ▸WKS.MANAGEMENT, ▸WKS.ADMIN-SERVICE.	▸peerCerts.tlsCert, ▸peerCerts.sigCert, ▸peerCerts.encCert	Der IssuerDN der SIG/ENC/TLS-Zertifikate stimmt überein.
6	Immer	▸peerCerts.tlsCert, ▸peerCerts.sigCert, ▸peerCerts.encCert	Die Zertifikate können über den Issuer (Sub-CA) ▸peerCerts bis zum im SMGW konfigurierten RootCA-Zertifikat validiert werden.
7	Immer	▸peerCerts.tlsCert, ▸peerCerts.sigCert, ▸peerCerts.encCert	Die Extended-KeyUsage und KeyUsage Extensions der Zertifikate entsprechen dem Zertifikatsprofil gemäß [TR-03109-4] für CTls(ENu), CSign(Enu) und CEnc(Enu) Zertifikate.

Nr.	Bedingung	Datenfeld	Prüfung
8	▸peerCerts.caCert ist vorhanden	▸peerCerts.caCert	Das Zertifikat im Datenfeld entspricht dem Zertifikatsprofil gemäß [TR-03109-4] für C(Sub-CA)-Zertifikate.
9	▸wks ist gleich ▸WKS.MANAGEMENT, ▸WKS.ADMIN-SERVICE, ▸WKS.NTP-TLS, ▸WKS.DOWNLOAD	▸peerCerts.tlsCert, ▸peerCerts.sigCert, ▸peerCerts.encCert	Die Public Keys GWA_WAN_TLS_PUB, GWA_WAN_SIG_PUB, GWA_WAN_ENC_PUB, stimmen mit den zuvor mittels ▸FA.DoImportGwaKeys in das Sicherheitsmodul importierten Schlüsseln überein.
10	▸wks ist gleich ▸WKS.INFO-REPORT und der SubjectCN des ▸peerCerts.tlsCert enthält die Funktion "gwa".	▸peerCerts.tlsCert, ▸peerCerts.encCert	Der SubjectCN des ENC-Zertifikates entspricht dem des ADMIN-SERVICE Kommunikationsprofils der Domäne "gwa". (Deprecated)
11	▸wks ist gleich ▸WKS.INFO-REPORT und der *SubjectCN* des ▸peerCerts.tlsCert enthält die Funktion "emt".	▸peerCerts.tlsCert, ▸peerCerts.encCert, ▸peerCerts.sigCert	Der SubjectDN der SIG/ENC/TLS-Zertifikate stimmt überein. Der IssueDN der SIG/ENC/TLS-Zertifikate stimmt überein.
12	▸wks ist gleich ▸WKS.TLS-PROXY	▸peerCerts.tlsCert	Der *SubjectCN* entspricht [SM-PKI-CP] Anhang A (SM-PKI) oder C (SM-Test-PKI) für die Funktion "emt".

Tabelle 3.52 Plausibilitätsprüfungen

ICS

ICS.FA.CreateWanComProfile.10

Der GWH **MUSS** im ICS deklarieren, welche Plausibilitätsprüfungen gemäß ▸Tabelle 3.46 das SMGW durchführt.

3.17.5 FA.UpdateWanComProfile

3.17.5.1 Beschreibung

Der FA erlaubt die Änderung der Kommunikationsparameter zur Kommunikation mit dem Kommunikationssystem eines bereits kommunikativ angebundenen GWA oder EMT.

Das SMGW überprüft, ob das als Aufrufparameter übergebene WAN-Kommunikationsprofil (▸Abschnitt 3.22.46) den aktuellen GWA identifiziert, plausibel ist und nur zulässige Datenfelder gegenüber dem persistierten WAN-Kommunikationsprofil geändert wurden.

3.17.5.2 Auslöser

REQ.FA.UpdateWanComProfile.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle SRV.

3.17.5.3 Anforderungen

- Das SMGW **SOLL** die Datenfelder gemäß ▸Tabelle 3.52 auf Plausibilität prüfen und im Fehlerfall den Import ablehnen. ▸ [FNN.20003.2] [REQ.FA.UpdateWanComProfile.20]
- Das SMGW **MUSS** den Import ablehnen, sofern Datenfelder gemäß ▸Tabelle 3.53 geändert würden. ▸ [FNN.20003.3] [REQ.FA.UpdateWanComProfile.30]
- Das SMGW **MUSS** für fehlende optionale Datenfelder im Aufrufparameter die entsprechenden bereits konfigurierten Daten unverändert lassen. [REQ.FA.UpdateWanComProfile.45]
- Das SMGW **MUSS** das Kommunikationsprofil persistieren und die Kommunikationsparameter künftig für die Kommunikation mit dem Kommunikationspartner für das WKS aus ▸wks verwenden. ▸ [BSI.20003.0] Für ▸WKS.NTP-TLS: ▸ [BSI.13009.0] [REQ.FA.UpdateWanComProfile.50]

Nr.	Bedingung	Datenfeld	Prüfung
1	▸wks ist gleich ▸WKS.MANAGEMENT, ▸WKS.ADMIN-SERVICE, ▸WKS.NTP-TLS, ▸WKS.DOWNLOAD.	▸peerCerts.tlsCert, ▸peerCerts.sigCert, ▸peerCerts.encCert im Aufrufparameter	Der *SubjectCN* der TLS/SIG/ENC Zertifikate entspricht den SubjectCN des im SMGW konfigurierten ▸peerCerts.tlsCert, ▸peerCerts.sigCert, ▸peerCerts.encCert des WAN-Kommunikationsprofils. Hinweis: Das Update der GWA-Zertifikate im WAN-Kommunikationsprofil ist mit einem Wechsel der Ressourcen-Domäne verbunden ("gwapre-management", "gwapre-adminservice", "gwapre-ntptls", "gwapre-download" → "gwa-management", "gwa-adminservice", "gwa-ntptls", "gwa-download")
2	Immer	▸wks im Aufrufparameter	Unverändert gegenüber dem im SMGW konfigurierten ▸wks
3	Aufruf über ▸HKS.WS1 mit Rolle SRV	▸peerCerts.tlsCert, ▸peerCerts.sigCert, ▸peerCerts.encCert im Aufrufparameter	Das Datenfeld muss leer sein, da der Servicetechniker keine Zertifikate ändern darf.
4	Aufruf über ▸HKS.WS1 mit Rolle SRV	▸wks im Aufrufparameter	Nur Profile vom Typ ▸WKS.MANAGEMENT, ▸WKS.ADMIN-SERVICE, ▸WKS.NTP-TLS, ▸WKS.DOWNLOAD dürfen geändert werden

Tabelle 3.53 Plausibilitätsprüfungen

3.17.6 FA.DeleteWanComProfile

3.17.6.1 Beschreibung

Das SMGW entfernt das im Aufruf identifizierte WAN-Kommunikationsprofil zur Kommunikation mit dem bisherigen EMT-Kommunikationssystem.

3.17.6.2 Auslöser



REQ.FA.DeleteWanComProfile.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.17.6.3 Anforderungen

- Das SMGW **MUSS** das Löschen ablehnen, wenn die referenzielle Integrität gemäß ▸Tabelle 3.54 nicht mehr gegeben wäre. ▸ [FNN.20004.1] [REQ.WAN.Kommunikationsprofil.60]
- Das SMGW **MUSS** das Kommunikationsprofil so löschen, dass es künftig nicht mehr zur Kommunikation verwendet werden kann. ▸ [FNN.20004.0] [REQ.FA.DeleteWanComProfile.20]

Nr.	Bedingung	Datenfeld	Prüfung
1	▸wks ist gleich ▸WKS.INFO-REPORT	▸meterDataOutput.wanPeerRef	Es existiert kein Auswertungsprofil dessen ▸meterDataOutput.wanPeerRef auf das zu löschende WAN-Kommunikationsprofil verweist und die Vorhaltefrist gemäß ▸Abschnitt 5.5 ist noch nicht abgelaufen.
2	▸wks ist gleich ▸WKS.TLS-PROXY	▸wanPeerRef	Es existiert kein Proxy-Kommunikationsprofil dessen ▸wanPeerRef auf das zu löschende WAN-Kommunikationsprofil verweist.

Tabelle 3.54 Plausibilitätsprüfungen

3.17.7 FA.ReadWanComProfile

3.17.7.1 Beschreibung

Das SMGW exportiert auf Anforderung das im Aufruf identifizierte WAN-Kommunikationsprofil. Dies kann ein EMT-WAN-Kommunikationsprofil oder ein GWA-WAN-Kommunikationsprofil sein.

3.17.7.2 Auslöser



REQ.FA.ReadWanComProfile.20

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT oder
- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle SRV.

3.17.7.3 Anforderungen

Das SMGW **MUSS** das im Aufrufparameter identifizierte WAN-Kommunikationsprofil (Siehe ▸Abschnitt 3.22.46) an den Aufrufer exportieren. ▸ [BSI.20031.0] [REQ.FA.ReadWanComProfile.10]

3.17.8 FA.DoRequestWanComTest

3.17.8.1 Beschreibung

Das SMGW löst einen TLS-Verbindungsaufbau zum WAN-Kommunikationspartner aus, dessen WAN-Kommunikationsprofil im Aufrufparameter über die Profil-ID eines WAN-Kommunikationsprofils identifiziert wird. Inhaltsdaten werden nicht übermittelt.

Das Ergebnis des Verbindungsaufbaus innerhalb einer im Aufrufparameter übergebenen Zeitspanne (Default: 30s) wird protokolliert und an den Aufrufer zurückgemeldet.

3.17.8.2 Auslöser



REQ.FA.DoRequestWanComTest.20

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.17.8.3 Anforderungen

Das SMGW **MUSS** einen TLS-Verbindungsaufbau mit dem über den Aufrufparameter ▸profileId identifizierten WAN-Kommunikationsprofil auslösen. [REQ.FA.DoRequestWanComTest.10] Die Verbindung wird gemäß Kommunikationsparametern im WAN-Kommunikationsprofil beendet.

3.17.9 FA.UpdateWanIfProfile

3.17.9.1 Beschreibung

Dieser Anwendungsfall ermöglicht die Änderung und Persistierung von Physical- und Link-Layer-Parametern einer Schnittstelle zur Kommunikation im WAN-Netzwerk:

- Konfigurationsparameter der physischen WAN-Schnittstelle zur Anmeldung an das WAN-Zugangsnetz (SIM-PIN, den Access-Point-Name oder die Access-Point-Credentials)
- Zuvor vom GWA konfigurierte WAN-Zugangsnetzparameter aktivieren
- Wake-Up-Port
- Parameter zur Bestimmung der SMGW WAN-Schnittstellen-Adresse
- Parameter zur Konfiguration der physischen und Link-Layer-Parameter der Schnittstelle

Es können nur Parameter von Schnittstellen geändert werden, die bereits zur Auslieferung vorhanden und konfiguriert sind. Bis dahin gelten die initialen Konfigurationsparameter.

3.17.9.2 Auslöser



REQ.FA.UpdateWanIfProfile.30

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle SRV.

3.17.9.3 Anforderungen

- Das SMGW **MUSS** die Aktualisierung ablehnen, wenn die Bezeichnung der Schnittstelle im Aufrufparameter ▸ifName nicht der im zu aktualisierenden Profil entspricht oder nicht mit "WAN" beginnt. [REQ.FA.UpdateWanIfProfile.20]
- Das SMGW **MUSS** für fehlende optionale Datenfelder im Aufrufparameter die entsprechenden bereits konfigurierten Daten unverändert lassen. [REQ.FA.UpdateWanIfProfile.25]
- Das SMGW **MUSS** das als Aufrufparameter übergebene ▸WAN-Schnittstellenkonfigurationsprofil persistieren und die Kommunikationsparameter künftig für die Kommunikation über die benannte WAN-Schnittstelle verwenden. [REQ.FA.UpdateWanIfProfile.10]

3.17.10 FA.UpdateHanIfProfile

3.17.10.1 Beschreibung

Dieser Anwendungsfall ermöglicht die Änderung und Persistierung von HAN-Schnittstellenparametern zur Kommunikation im HAN-Netzwerk. Dazu gehören die IP-Adressen der Schnittstelle und der Bereich der IP-Adressen des Netzwerkes und die Ports der Dienste des SMGW.

Die Änderungen werden ggf. erst nach einem Neustart des SMGW gültig.

Bis zur ersten Änderung gelten die initialen Konfigurationsparameter.

Dieser FA erlaubt die Änderung folgender Parameter:

- Parameter zur Begrenzung ungültiger Authentifizierungsversuche gegen Brute-Force-Angriffe
- Parameter zur Bestimmung der SMGW HAN-Schnittstellen-Adresse
- Parameter zur Bestimmung der Portnummern für die Dienste (HKS) des SMGW
- Parameter zur Konfiguration der physischen und Link-Layer-Parameter der Schnittstelle

Sofern die Implementierung mehrere HAN-Schnittstellen mit getrennten Netzwerken unterstützt, werden diese als HAN-CON und HAN-CLS bezeichneten Schnittstellen individuell konfiguriert. Für jede Schnittstelle sind individuelle Parameter konfigurierbar.

Sofern die Implementierung nur ein HAN-Netzwerk unterstützt, wird diese Schnittstelle als HAN bezeichnet.

3.17.10.2 Auslöser



REQ.FA.UpdateHanIfProfile.30

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.17.10.3 Anforderungen

- Das SMGW **MUSS** die Aktualisierung ablehnen, wenn die Bezeichnung der Schnittstelle im Aufrufparameter ▸ifName nicht der im zu aktualisierenden Profil entspricht oder nicht mit "HAN" beginnt. [REQ.FA.UpdateHanIfProfile.20]
- Das SMGW **MUSS** die Aktualisierung ablehnen, wenn der ▸hostIpv4Addr.mode "static" gewählt wurde, ▸hostIpv4Addr.ip4Addr gemäß [RFC1918] keine private Adresse ist oder die Subnetz-Maske ▸hostIpv4Addr.ip4Mask nicht gültig ist. [REQ.FA.UpdateHanIfProfile.40] Gültige Subnetzmasken besitzen eine Folge von 0-32 "1" Bits gefolgt von einer Folge von 0-32 "0" Bits mit einer Gesamtlänge von 32 Bits (anzugeben in Dotted-Decimal-Repräsentation der vier Octets).
- Das SMGW **MUSS** für fehlende optionale Datenfelder im Aufrufparameter die entsprechenden bereits konfigurierten Daten unverändert lassen. [REQ.FA.UpdateHanIfProfile.45]

- Das SMGW **MUSS** das als Aufrufparameter übergebene ▸HAN-Schnittstellenkonfigurationsprofil persistieren und die Kommunikationsparameter künftig für die Kommunikation über die benannte HAN-Schnittstelle verwenden. [REQ.FA.UpdateHanIfProfile.10]

ICS



ICS.FA.UpdateHanIfProfile.10

Der GWH **MUSS** im ICS deklarieren, ob die Änderungen der IP-Adresse und der Dienste unmittelbar (true) oder erst nach einem Neustart (false) wirksam sind.

3.17.11 FA.UpdateLmnIfProfile

3.17.11.1 Beschreibung

Dieser Anwendungsfall ermöglicht die Änderung und Persistierung von LMN-Schnittstellenparametern zur Kommunikation im LMN.

Es können nur Parameter von Schnittstellen geändert werden, die bereits zur Auslieferung vorhanden und konfiguriert sind. Bis dahin gelten die initialen Konfigurationsparameter.

Dieser FA erlaubt die Änderung herstellerspezifischer Parameter zur Konfiguration der physischen und Link-Layer-Parameter der LMN-Schnittstelle.

3.17.11.2 Auslöser



REQ.FA.UpdateLmnIfProfile.30

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.17.11.3 Anforderungen

- Das SMGW **MUSS** die Aktualisierung ablehnen, wenn die Bezeichnung der Schnittstelle im Aufrufparameter ▸ifName nicht der im zu aktualisierenden Profil entspricht oder nicht mit "LMN" beginnt. [REQ.FA.UpdateLmnIfProfile.20]
- Das SMGW **MUSS** das als Aufrufparameter übergebene ▸LMN-Schnittstellenkonfigurationsprofil persistieren und die Kommunikationsparameter künftig für die Kommunikation über die benannte LMN-Schnittstelle verwenden. [REQ.FA.UpdateLmnIfProfile.10]

3.17.12 FA.DoImportGwaKeys

3.17.12.1 Beschreibung

Der FA ermöglicht die Aktualisierung der öffentlichen Schlüssel des GWA im Sicherheitsmodul unter Verwendung der vom GWA erzeugten CV-Import-Zertifikate (siehe ▸Abschnitt 3.22.20).

Das Sicherheitsmodul besitzt zwei GWA-Schlüsselsätze mit jeweils vier Schlüsselobjekte (TLS, SIG, ENC, AUT).

Der GWA benötigt zur Erstellung der CV-Import-Zertifikate die Schlüsselreferenzen freier Schlüsselobjekte im Sicherheitsmodul. Diese erhält er über ▸FA.DoPrepareImportGwaKeys.

Die bisherigen Schlüssel und Zertifikate GWA_WAN_TLS_CRT$_{n-1}$, GWA_WAN_SIG_CRT$_{n-1}$, GWA_WAN_ENC_CRT$_{n-1}$ können anschließend durch ▸FA.DoDeactivateGwaCerts deaktiviert werden.

Aus diesem Grund ist ein kontrollierter Betriebsprozess zum Wechsel der GWA-Zertifikate im Zusammenspiel mit dem GWA Backendsystemen notwendig. Solange der bisherige Schlüssel und das Zertifikat GWA_WAN_TLS_CRT$_{n-1}$ noch im (Sicherheitsmodul des) SMGW aktiv ist, kann es für die TLS-Authentifizierung des GWA verwendet werden. Solange der bisherige Schlüssel und das Zertifikat GWA_WAN_ENC_CRT$_{n-1}$ noch im (Sicherheitsmodul des) SMGW aktiv ist, kann es für die Verschlüsselung von Inhaltsdaten-Nachrichten an den GWA verwendet werden. Solange der bisherige Schlüssel und das Zertifikat GWA_WAN_SIG_CRT$_{n-1}$ noch im (Sicherheitsmodul des) SMGW aktiv ist, kann es für die Validierung von Inhaltsdaten-Nachrichten des GWA verwendet werden.

Der GWA muss am Sicherheitsmodul authentifiziert sein.

3.17.12.2 Auslöser



REQ.FA.DoImportGwaKeys.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.17.12.3 Anforderungen

- Das SMGW **MUSS** den Import ablehnen, wenn mindestens eines der Datenfelder ▸tlsKeyCvCert, ▸sigKeyCvCert, ▸encKeyCvCert, ▸autKeyCvCert nicht vorhanden oder ungültig ist. ▸ [BSI.4009.1] [REQ.FA.DoImportGwaKeys.20]
- Das SMGW **MUSS** die im Aufrufparameter übergebenen CV-Zertifikate in die Schlüsselobjekte des Sicherheitsmoduls importieren, die für die künftige GWA-Kommunikation vorgesehen sind ("GWAPRE"). ▸ [BSI.4009.0] ▸ [BSI.4009.2] [REQ.FA.DoImportGwaKeys.30]

3.17.12.4 Implementierungshinweise

Werden neue GWA-Zertifikate importiert, müssen die öffentlichen Schlüssel aus den GWA-Zertifikaten in das Sicherheitsmodul importiert (siehe [TR-03109-2] UC_PN_04_04) werden. Das SMGW verwendet die Import-Zertifikate des Aufrufparameters zum Import der den Zertifikaten entsprechenden öffentlichen Schlüssel GWA_WAN_TLS_PUB, GWA_WAN_SIG_PUB, GWA_WAN_ENC_PUB in die entsprechenden Schlüsselobjekte des Sicherheitsmodules.

Der Schlüssel GWA_WAN_TLS_PUB wird ergänzend auch als GWA_WAN_TLS_AUT für die Authentifizierung des GWA am Sicherheitsmodul (Siehe ▸FA.DoRequestSecmodAuth) in das Sicherheitsmodul importiert.

3.17.13 FA.DoPrepareImportGwaKeys

3.17.13.1 Beschreibung

Dieser FA übermittelt dem Aufrufer die für die Erzeugung der GWA-Importzertifikate erforderlichen Schlüsselreferenzen zum nachfolgenden Import der GWA-Schlüssel (siehe ▸FA.DoImportGwaKeys).

3.17.13.2 Auslöser



REQ.FA.DoPrepareImportGwaKeys.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.17.13.3 Anforderungen

Das SMGW **MUSS** dem Aufrufer die GWA_TLS, GWA_ENC, GWA_SIG, GWA_AUT der für den Import der GWA-Schlüssel vorgesehenen Schlüsselobjekte als ▸Schlüsselreferenzen übermitteln. [REQ.FA.DoPrepareImportGwaKeys.20]

3.17.14 FA.DoDeactivateGwaCerts

3.17.14.1 Beschreibung

Das SMGW deaktiviert die nicht mehr verwendeten Schlüssel und Zertifikate GWA_WAN_TLS_PUB/CRT_{n-1}, GWA_WAN_ENC_PUB/CRT_{n-1} und GWA_WAN_SIG_PUB/CRT_{n-1} atomar, so dass sie nicht mehr zur Kommunikation, Verschlüsselung, Signatur verwendet werden können.

Der GWA muss dazu am Sicherheitsmodul authentifiziert sein.

3.17.14.2 Auslöser



REQ.FA.DoDeactivateGwaCerts.30

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.17.14.3 Anforderungen

- Das SMGW **MUSS** die Deaktivierung ablehnen, wenn vor der Deaktivierung nur noch ein aktiver GWA-Schlüssel/Zertifikatsatz im SMGW vorhanden ist. ▸ [FNN.17024.1] [REQ.FA.DoDeactivateGwaCerts.10]
- Das SMGW **MUSS** die Deaktivierung ablehnen, wenn die nach der Deaktivierung verbleibenden GWA-Schlüssel/Zertifikate noch nicht für eine Signaturprüfung, TLS-Verbindungsaufbau und Authentifizierung am Sicherheitsmodul erfolgreich verwendet wurden. [REQ.FA.DoDeactivateGwaCerts.15] Dies setzt die Nutzung von Wake-Up mit anschließendem TLS-Verbindungsaufbau für WKS.MANAGEMENT und Authentifizierung am Sicherheitsmodul voraus.
- Das SMGW **MUSS** die ältesten GWA_WAN_TLS_CRT$_{n-1}$, GWA_WAN_SIG_CRT$_{n-1}$, GWA_WAN_ENC_CRT$_{n-1}$ und die zugehörigen Schlüssel so deaktivieren, dass sich nicht mehr für die Kommunikation und Authentifizierung am Sicherheitsmodul verwendet werden können. ▸ [FNN.17024.0] [REQ.FA.DoDeactivateGwaCerts.20]

3.17.15 FA.DoRequestSecmodAuth

3.17.15.1 Beschreibung

Das Sicherheitsmodul des SMGW erzeugt eine Zufallszahl ("challenge") und das SMGW übermittelt diese an den GWA zur Authentifizierung des GWA am Sicherheitsmodul mittels ▸FA.DoResponseSecmodAuth.

3.17.15.2 Auslöser



REQ.FA.DoRequestSecmodAuth.30

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.17.15.3 Anforderungen

Das SMGW **MUSS** die Anforderung ablehnen, wenn sich das Sicherheitsmodul bereits im AUTH-Zustand befindet. ▸ [FNN.11001.2] [REQ.FA.DoRequestSecmodAuth.20]

Das SMGW **MUSS** das Sicherheitsmodul auffordern, eine Zufallszahl zu erzeugen und diese zusammen mit den vom SMGW für die im Sicherheitsmodul gespeicherten GWA_WAN_AUT_PUB unterstützten Algorithmen an den Aufrufer zurückgeben (siehe ▸AuthChallenge-Datenstrukturen). ▸ [FNN.11001.0] ▸ [FNN.11001.1] [REQ.FA.DoRequestSecmodAuth.10]

3.17.15.4 Implementierungshinweise

Die Funktionalität des Sicherheitsmodules (SM) gemäß [TR-03109-2] (Siehe UC_PN_04_02) bedingt, dass die vom SM erzeugte Zufallszahl temporär im SM gespeichert wird. Zwischen dem Erzeugen der ▸challenge und dem Verifizieren des ▸token durch das SM darf das SM keine weitere Zufallszahl erzeugen. Dies ist insbesondere bei der Verwendung des Sicherheitsmodules für die CMS-Inhaltsdatensicherung zu beachten.

Gemäß [TR-03109-2] benötigt das EXTERNAL AUTHENTICATE Kommando des Sicherheitsmodules eine 16 Byte Zufallszahl.

3.17.16 FA.DoResponseSecmodAuth

3.17.16.1 Beschreibung

Die Verwaltung des im SMGW integrierten Sicherheitsmodules (SM) ist nur im Zustand AUTH (siehe [TR-03109-2]) möglich. Das SM kann nur in den AUTH Zustand gebracht werden, indem ein Challenge-Response-Authentisierungsverfahren den GWA authentisiert. Dazu wird der im SM vorliegenden Schlüssel

GWA_WAN_AUT_PUB, welcher inhaltlich mit dem *GWA_WAN_TLS_PUB* identisch ist, und der beim GWA vorliegenden GWA_WAN_TLS_PRV verwendet.

Der AUTH Zustand ist Voraussetzung für die FAs zur Schlüsselpaarerzeugung der LMN-, HAN- und WAN-Schnittstelle und des Imports von öffentlichen Schlüsseln zu SM-PKI-Zertifikaten in das Sicherheitsmodul.

Mit diesem FA übermittelt der GWA dem SMGW die mit dem privaten Schlüssel GWA_WAN_TLS_PRV signierte Antwort (Response) an das SMGW. Das Sicherheitsmodul validiert das Token in der Antwort mit dem im Sicherheitsmodul gespeicherten zugehörigen öffentlichen Schlüssel und wechselt im Erfolgsfall in den AUTH Zustand.

Im SM können zwei Schlüssel ("GWAPRE": $GWA_WAN_AUT_PUB_{n+1}$ und "GWA": $GWA_WAN_AUT_PUB_{n}$) gleichzeitig gespeichert sein. Gründe sind:

- Erneuern des GWA-Zertifikatssatzes (alter und neuer Schlüssel)
- Laufender GWA-Wechselprozess (Schlüssel für neuen und alten GWA)

Aus diesem Grund muss der GWA dem SMGW bei der Übermittlung des "tokens" mitteilen, welchen Schlüssel er für die Authentifizierung verwendet.

Um die kryptografische Agilität des Authentifizierungsverfahrens zu ermöglichen, können SMGW und GWA die verwendbaren Verfahren vereinbaren und auswählen.

Das SMGW vermittelt in diesem FA als Authentisierungs-Proxy die Challenge-Response-Nachrichten zwischen SM und GWA.

Dieser FA setzt voraus, dass die unmittelbar zuvor über ▸FA.DoRequestSecmodAuth erzeugte Zufallszahl (challenge) in die Berechnung der Response eingeflossen ist. Zum Ablauf siehe ▸Abbildung 3.19.

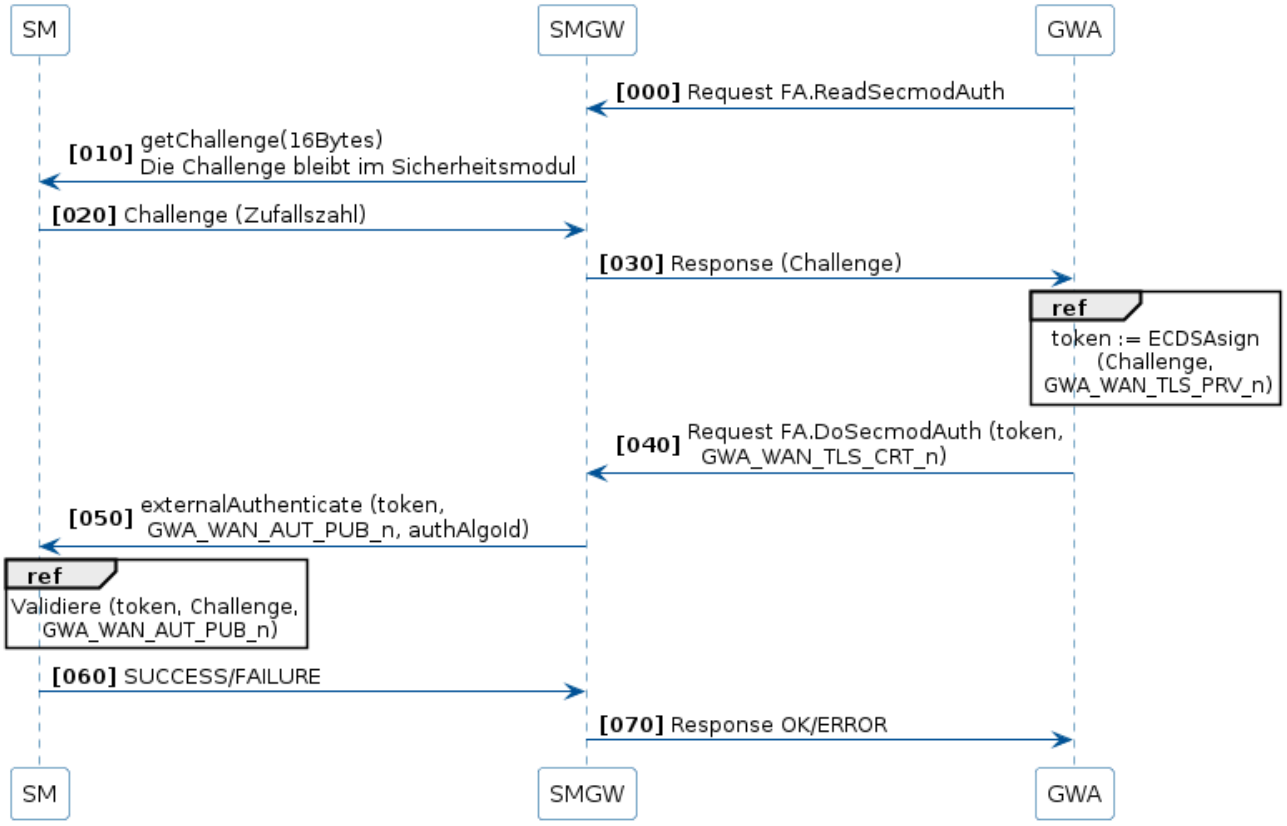


Abbildung 3.19. Übersicht über den Ablauf der GWA-Authentifizierung am Sicherheitsmodul des SMGW

3.17.16.2 Auslöser

REQ.FA.DoResponseSecmodAuth.60

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.17.16.3 Anforderungen

Das SMGW **MUSS** die Anforderung ablehnen, wenn sich das Sicherheitsmodul bereits im AUTH-Zustand befindet. ▸ [FNN.11002.3] [REQ.FA.DoResponseSecmodAuth.10]

Das SMGW **MUSS** den Aufruf ablehnen, wenn der Authentifizierungsalgorithmus ▸authAlgo nicht vom SMGW und mindestens einem im Sicherheitsmodul gespeicherten GWA_WAN_AUT_PUB unterstützt wird. ▸ [FNN.11002.3] [REQ.FA.DoResponseSecmodAuth.20]

Sofern im Aufrufparameter kein Hinweis ▸authCert zum Authentifizierungsschlüssel vorhanden ist, **MUSS** das SMGW die Validierung des ▸token mit dem GW_WAN_TLS_PUB der WKS-MANAGEMENT-Verbindung durchführen (dieser entspricht dem GW_WAN_AUT_PUB im Sicherheitsmodul). ▸ [FNN.11002.3] [REQ.FA.DoResponseSecmodAuth.50]

Das SMGW **MUSS** die Anforderung ablehnen, sofern der öffentliche Schlüssel des TLS-Zertifikates ▸authCert im Aufrufparameter nicht mit dem GWA_WAN_AUT_PUB des SM im SMGW übereinstimmt. ▸ [FNN.11002.2] [REQ.FA.DoResponseSecmodAuth.55]

Das SMGW **MUSS** das Ergebnis der Validierung des ▸token mit GWA_WAN_AUT_PUB durch das Sicherheitsmodul an den Aufrufer übermitteln. ▸ [FNN.11002.0] ▸ [FNN.11002.3] [REQ.FA.DoResponseSecmodAuth.30]

3.17.16.4 Implementierungshinweise

Gemäß [TR-03109-2] setzen die folgenden FAs voraus, dass der GWA am Sicherheitsmodul authentifiziert ist:

- ▸FA.DoDeactivateGwaCerts
- ▸FA.DoImportGwaKeys
- ▸FA.DoCreateSelfsignedSmgwHanCert
- ▸FA.DoCreateSelfsignedSmgwLmnCert
- ▸FA.DoDeactivateRootCaCert
- ▸FA.DoDeactivateSelfsignedSmgwHanCert
- ▸FA.DoDeactivateSelfsignedSmgwLmnCert
- ▸FA.DoDeactivateSmgwPkiCerts
- ▸FA.DoImportRootCaCert
- ▸FA.DoPrepareSecmod
- ▸FA.DoSmgwPkiCertRequest
- ▸FA.AcceptSwitchGwa

3.17.17 FA.DoFinishSecmodAuth

3.17.17.1 Beschreibung

Die Authentifizierung des GWA am Sicherheitsmodul des SMGW wird beendet.

Anschließend ist bis zum Aufruf von ▸Abschnitt 3.17.15 kein Schlüsselimport in das Sicherheitsmodul mehr möglich.

3.17.17.2 Auslöser



REQ.FA.DoFinishSecmodAuth.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- 10 Minuten nach Empfang eines AUTH-Zustand erfordernden Kommandos.
- Bei Aufruf von ▸FA.DoSwitchGwa

3.17.17.3 Anforderungen

Das SMGW **MUSS** den AUTH-Zustand des Sicherheitsmodules so beenden, dass für den Aufruf der in ▸FA.DoResponseSecmodAuth genannten FAs eine erneute Authentifizierung des GWA am Sicherheitsmodul erforderlich ist. [REQ.FA.DoFinishSecmodAuth.20]

3.17.18 FA.InitiateManagementConnection

3.17.18.1 Beschreibung

Dieser FA wird aufgerufen, sofern eine gültige Wake-Up-Nachricht (Version 1) eintrifft, die mit dem im Sicherheitsmodul gespeicherten, öffentlichen Signaturschlüssel des aktuellen GWA validiert werden kann. Sofern eine Management-Verbindung besteht, wird diese beendet. Damit wird die Möglichkeit gegeben, eine einseitig bestehende,[13] nicht mehr verwendbare Verbindung abzubauen und das SMGW zu veranlassen, eine Verbindung erneut aufzubauen.

Das SMGW initiiert den Aufbau der Management-Verbindung mit den Kommunikationsparametern des WAN-Kommunikationsprofils der Domäne "gwa-management" (Aktueller GWA).

3.17.18.2 Auslöser

REQ.WAN.Kommunikationsszenarien.110

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer mit dem GWA_WAN_SIG_PUB validierten gültigen Wake-Up-Nachricht über ▸WKS.WAKEUP.

▸ [BSI.7001.0]

3.17.18.3 Anforderungen

- Das SMGW **MUSS** eine bestehende WKS.MANAGEMENT Verbindung zunächst beenden. [REQ.FA.InitiateManagementConnection.10]
- Das SMGW **MUSS** innerhalb von 20 Sekunden eine Verbindung über ▸WKS.MANAGEMENT mit den Kommunikationsparametern ▸outboundConnection aus dem WAN-Kommunikationsprofil mit der ProfileId zu "gwa-management" initiieren. [REQ.WKS.WakeUp.20]

3.17.19 FA.DoReboot

3.17.19.1 Beschreibung

Ein Neustart des SMGW wird angefordert.

3.17.19.2 Auslöser

REQ.FA.DoReboot.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Wiederkehr der Spannungsversorgung nach einem Ausfall der Spannungsversorgung des SMGW.
- Empfang einer Anfrage zum Neustart über ▸WKS.MANAGEMENT.
- Empfang einer Anfrage zum Neustart über ▸HKS.WS1 in der Rolle SRV.

3.17.19.3 Anforderungen

Das SMGW **MUSS** innerhalb der Zeit ▸ICS.FA.DoReboot.10 einen Neustart durchführen und für die Verarbeitung einer Wake-Up-Nachricht bereit sein. ▸ [FNN.6005.0] [REQ.FA.DoReboot.20]

ICS

[13] Einer der Kommunikationspartner ist nicht im Zustand "TCP/TLS-Connection closed".



ICS.FA.DoReboot.10

Der GWH **MUSS** im ICS beschreiben, wie lange das SMGW nach Auslösen des FA benötigt (in Sekunden), bis das SMGW für die Verarbeitung einer Wake-Up-Nachricht bereit ist. Der Wert muss kleiner als 600 Sekunden sein.

3.17.20 FA.DoDeleteUserData

3.17.20.1 Beschreibung

Das SMGW verhindert unwiderruflich den Zugriff auf alle personenbezogenen Daten, die zum Aufrufzeitpunkt im SMGW gespeichert sind.

So kann das SMGW künftig zum Ausbau, zur Wiederaufbereitung, zum Neueinbau transportiert und verwendet werden.

Zu den Daten gehören historische Daten aller mit Verarbeitungsprofilen verbundenen Messwertlisten (bspw. AWL, RWL, TWL), letzte empfangene (aktuelle) Messwerte, Logbücher, sowie die Verarbeitungsprofile und die damit verknüpften Konfigurationsprofile zur kommunikativen Anbindung von Zähler, HAN-Usern (Anschlussnutzer/Anlagenbetreiber) und EMT.

Darüber hinaus werden die Proxy-Kommunikationsprofile gelöscht.

Dabei werden alle Vorhaltefristen außer Kraft gesetzt. Sofern es Anforderungen an Aufbewahrungsfristen gibt, müssen die Daten zuvor exportiert worden sein und außerhalb des SMGW aufbewahrt werden.



Warnung

Werden im Rahmen dieses FA Daten gelöscht, ist zu beachten, dass die eichrechtlichen Fristen durch geeignete Aufbewahrung in signierter Form außerhalb des SMGW sichergestellt werden müssen. Da der GWA keinen Zugriff auf Messwertlisten und Anschlussnutzer-Logs hat, muss den betroffenen Anschlussnutzern hierbei die Gelegenheit gegeben werden, diese Daten exportieren zu können.

3.17.20.2 Auslöser



REQ.FA.DoDeleteUserData.30

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Empfang einer Anfrage über ▸HKS.WS1 in der Rolle SRV.

3.17.20.3 Anforderungen



REQ.FA.DoDeleteUserData.10

Das SMGW **MUSS** nach dem Ausführen des FA bis zum erneuten Anlegen der Profile den Lese-Zugriff auf Inhalte der folgende Ressourcen bzw. Datenobjekte mit Fehler ablehnen:

- Auswertungsprofile (processingProfile)
- LMN-Kommunikationsprofile (Zählerprofile)
- HAN-Kommunikationsprofile der Rolle CON und CLS
- EMT-WAN-Kommunikationsprofile
- Proxy-Kommunikationsprofile
- Weitere Daten gemäß ▸ICS.FA.DoDeleteUserData.10



REQ.FA.DoDeleteUserData.20

Das SMGW **MUSS** den Lese-Zugriff auf Inhalte, die vor dem Aufruf des FA in den folgenden Datenobjekten gespeichert waren, mit Fehler ablehnen:

- Alle AWL
- Alle RWL
- Alle TWL
- Anschlussnutzer-Logs
- System-Log
- Eichlog mit Ausnahme der folgenden Einträge: erkannte Integritätsfehler (▸ [BSI.19001.1]), erfolgreiche Firmware-Updates (▸ [BSI.18009.0]), dauerhafte Störung der Sicherheitsfunktionalität (▸ [BSI.4010.2])
- Weitere Daten gemäß ▸ICS.FA.DoDeleteUserData.10

Das SMGW **MUSS** die Ausführung des FA protokollieren. ▸ [BSI.19019.0] ▸ [BSI.19019.1] [REQ.FA.DoDeleteUserData.40]

ICS



ICS.FA.DoDeleteUserData.10

Der GWH **MUSS** im ICS beschreiben, auf welche weiteren personenbezogenen Ressourcen/Datenobjekte an den Schnittstellen des SMGW zugegriffen werden kann. Für diese Ressourcen ist zu beschreiben, wie der Zugriff erfolgt.

3.17.20.4 Implementierungshinweise

Die Implementierung soll die Daten zuverlässig löschen. Sofern die Daten mit einem kryptografischen Verfahren nach Stand der Technik verschlüsselt persistiert sind, ist auch das Löschen des Schlüssels zur Entschlüsselung der persistierten Daten möglich.

3.18 GWA-Wechsel (FAKAT.GwaSwitch)

3.18.1 Übersicht

Die Anwendungsfälle dieser Kategorie beschreiben die Funktionalität des SMGW zur Unterstützung eines GWA-Wechselprozesses und des GWA-Zertifikatswechselprozesses.

Die Wechselprozesse zwischen zwei GWA und der GWA-Zertifikate werden in [TR-03109-1-VI] beschrieben.

Die FA sind so beschrieben, dass durch das Verhalten des SMGW ein zuverlässiger Wechsel von einem GWA-Zertifikatssatz und Satz von GWA-WAN-Kommunikationsprofilen auf einen weiteren Satz Zertifikate bzw. Kommunikationssystem erfolgt.

In diesem Kapitel werden Zertifikats-Datenobjekte im Rahmen von Wechsel- oder Aktualisierungsprozessen mit einem Suffix n gekennzeichnet, welches die zeitliche Abfolge der Verwendung des Zertifikates ordnet. Dabei bezeichnet n-1 ein künftig nicht mehr zu verwendendes Zertifikat und n+1 das künftige Zertifikat.

3.18.2 Übersicht der FA

Aufgabe	Umsetzung
Neue GWA-Schlüssel, Zertifikate und Konfiguration für neuen GWA importieren (in der Domäne "gwapre")	Durch den GWA im Wechselprozess gesteuerter Ablauf: Das SMGW **MUSS** ▸FA.DoPrepareImportGwaKeys für den GWA umsetzen. [REQ.WAN.Management.191] Das SMGW setzt ▸FA.DoImportGwaKeys für den GWA um. Das SMGW **MUSS** ▸FA.UpdateWanComProfile für den GWA mit der Ressourcen-Domäne "gwapre" umsetzen. [REQ.WAN.Management.230]
Wechsel der GWA-Schlüssel und Kommunikationsparameter auslösen	Das SMGW **MUSS** ▸FA.DoSwitchGwa für den GWA umsetzen. [REQ.WAN.Management.231]

Aufgabe	Umsetzung
Wechsel der GWA-Schlüssel und Kommunikationsparameter bestätigen	Das SMGW **MUSS** ▸FA.AcceptSwitchGwa für den GWA umsetzen. [REQ.FAKAT.GwaSwitch.20]

Tabelle 3.55 Übersicht der FA der Kategorie FAKAT.GwaSwitch

3.18.3 Datenstrukturen der FA-Kategorie

Die Datenstruktur mit den Parametern für den GWA-Wechsel ist in ▸Abschnitt 3.22.19 beschrieben.

3.18.4 FA.DoSwitchGwa

3.18.4.1 Beschreibung

Nach Prüfung der Voraussetzungen für einen GWA-Wechselprozess im SMGW verwendet das SMGW nach Ausführung dieses FA für die Kommunikation mit dem GWA die Schlüssel, Zertifikate und Kommunikationsparameter des künftigen GWA-Kommunikationssystems.

Über Aufrufparameter (siehe ▸GWA-Wechselparameter) kann der Wechselzeitpunkt und die maximale Dauer bis zum Empfang der Bestätigung über ▸FA.AcceptSwitchGwa festgelegt werden.

Nach erfolgreicher Kommunikation mit dem künftigen GWA (siehe ▸FA.AcceptSwitchGwa) können die bisherigen GWA-Schlüssel des bisherigen GWA durch den künftigen GWA gelöscht werden. (▸FA.DoDeactivateGwaCerts).

3.18.4.2 Auslöser



REQ.FA.DoSwitchGwa.40

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.18.4.3 Anforderungen

- Das SMGW **MUSS** den Aufruf ablehnen, wenn die GWA-Schlüsselbank für den Wechsel im Sicherheitsmodul nicht aktiviert ist oder die Schlüssel der Zertifikate der WAN-Kommunikationsprofile gwapre-adminservice, gwapre-management, gwapre-ntptls nicht damit übereinstimmen. [REQ.FA.DoSwitchGwa.10]
- Das SMGW **MUSS** alle noch bestehenden TLS-Verbindungen zum GWA beenden. [REQ.FA.DoSwitchGwa.50]
- Das SMGW **MUSS** eine evtl. noch bestehende Authentifizierung am Sicherheitsmodul beenden. [REQ.FA.DoSwitchGwa.60]
- Das SMGW **MUSS** den Verbindungsaufbau über ▸WKS.ADMIN-SERVICE zum künftigen GWA innerhalb von 60 Sekunden nach dem im Aufrufparameter angegebenen Zeitpunkt ▸switchTime beginnen ▸ [FNN.17023.0] . [REQ.FA.DoSwitchGwa.20]
- Das SMGW **MUSS** den GWA-Wechsel abbrechen, wenn nicht innerhalb der im Aufrufparameter angegeben Zeitdauer ▸switchTimeout eine Bestätigung durch ▸FA.AcceptSwitchGwa ausgelöst wurde. ▸ [FNN.17023.1] [REQ.FA.DoSwitchGwa.30]

3.18.5 FA.AcceptSwitchGwa

3.18.5.1 Beschreibung

Der Wechselprozess auf den neuen GWA-Schlüsselsatz und die WAN-Kommunikationsparameter war erfolgreich. Der GWA konnte sich erfolgreich am Sicherheitsmodul authentisieren. Die bisherigen GWA-Schlüssel, Zertifikate und WAN-Kommunikationsprofile werden nicht mehr benötigt.

Sofern der GWA nicht innerhalb einer festgelegten Zeit ("Wechseltimeout") die Authentifizierung am Sicherheitsmodul mit dem neuen GWA_WAN_AUT_PUB durchführt, wird der Wechselprozess abgebrochen und der Schlüsselsatz des bisherigen GWA wird weiterhin verwendet. Die WAN-Kommunikationsprofile "gwa-

management", "gwa-adminservice", "gwa-ntptls" enthalten weiterhin die Kommunikationsparameter des bisherigen GWA.

3.18.5.2 Auslöser

Das SMGW **MUSS** den FA nach erfolgreicher Ausführung des ▸FA.DoResponseSecmodAuth durch den künftigen GWA (Authentifizierung mit GWA_WAN_SIG_CRT$_{n+1}$) auslösen. [REQ.FA.AcceptSwitchGwa.10]

3.18.5.3 Anforderungen

- Das SMGW **MUSS** nach erstmaliger Authentifizierung mit einem GWA_WAN_AUT_PUB (entspricht GWA_WAN_TLS_PUB zum "gwapre"-WAN-Kommunikationsprofil) den GWA-Wechsel erfolgreich beenden. ▸ [FNN.17017.0] [REQ.FA.AcceptSwitchGwa.30]

3.19 Verwaltung der SMGW-Zertifikate (FAKAT.SmgwCertMgmt)

3.19.1 Übersicht

Die Anwendungsfälle dieser Kategorie beschreiben die Funktionalität zur Verwaltung der SMGW-Zertifikate. Dazu gehört die Erneuerung der SM-PKI-Zertifikate und weiterer Gerätezertifikate.

Die Anwendungsfälle unterstützen den GWA bei der Verwaltung der Zertifikate des SMGW, d.h. das Einbringen, Entfernen und das rechtzeitige Erneuern der Zertifikate der SM-PKI. Das SMGW übernimmt dabei die Erstellung und Speicherung der Schlüsselpaare und Zertifikats-Signatur-Anforderungen (CSR). Das SMGW kann selbst keine Zertifikate oder Sperrlistenprüfungen durchführen. Entsprechend beantragt der GWA - stellvertretend für das SMGW - die Zertifikate und führt die Sperrlistenprüfungen durch. Das SMGW löscht Zertifikate nicht selbstständig.

Der Wechsel der Zertifikate setzt ein Zusammenspiel von SMGW und GWA voraus (siehe dazu Betriebsprozesse [TR-03109-1-VI]). Das SMGW prüft die inhaltliche Gültigkeit der Zertifikate für die vom SMGW verwendeten Zertifikatsfelder, die zeitliche Gültigkeit und ob die verwendeten Eigenschaften des Zertifikates (beispielsweise kryptographische Verfahren) vom SMGW unterstützt werden.

Die FAs sind so beschrieben, dass durch das Verhalten des SMGW eine Ausfallsicherheit beim Zertifikatswechsel von GWA- und SMGW-Zertifikate gegeben ist. Wesentliche Voraussetzung für die Ausfallsicherheit bei Zertifikatswechselprozessen des SMGW ist die Fähigkeit, für die WAN-, LMN- und HAN-Schnittstelle jeweils zwei Sätze[14] für Schlüsselpaare und Zertifikate persistieren zu können.

Ein Wechsel des SMGW zwischen SM-PKI und SM-Test-PKI ist nicht möglich.

Bei der Vor-Personalisierung erhält das SMGW über den GWH sogenannte Gütesiegelzertifikate (GW_WAN_TLS/SIG/ENC_CRT$_0$). Diese werden bei der Personalisierung und dem Übergang in den Wirkbetrieb durch den GWA durch die ersten Wirkzertifikate aktualisiert. Der Übergang in den Wirkbetrieb wird als Erst-Inbetriebnahme im Eichlog protokolliert.

In diesem Kapitel werden Zertifikats-Datenobjekte im Rahmen von Wechsel- oder Aktualisierungsprozessen mit einem Suffix n gekennzeichnet, welches die zeitliche Abfolge der Verwendung des Zertifikates ordnet. Dabei bezeichnet n-1 ein künftig nicht mehr zu verwendendes Zertifikat und n+1 das künftige Zertifikat.

3.19.2 Übersicht der FA

Aufgabe	Umsetzung
WAN (SM-PKI)	
Auslesen der im SMGW gespeicherten Vertrauensanker- und SMGW-Zertifikate durch GWA	Das SMGW **MUSS+** ▸FA.ReadCertificate für den GWA umsetzen. [REQ.WAN.Management.193]
Erzeugen des Schlüsselobjektes für den Import eines RootCA-Zertifikates durch den GWA	Das SMGW **MUSS** ▸FA.DoPrepareImportRootCaKey für den GWA umsetzen. [REQ.WAN.Management.182]

[14] Im Sicherheitsmodul auch "Schlüsselbänke" genannt.

Aufgabe	Umsetzung
Import von RootCA-Zertifikaten durch den GWA	Das SMGW **MUSS** ▸FA.DoImportRootCaCert für den GWA umsetzen. [REQ.WAN.Management.180]
Löschen von RootCA-Zertifikaten durch den GWA	Das SMGW **MUSS** ▸FA.DoDeactivateRootCaCert für den GWA umsetzen. [REQ.WAN.Management.181]
Erzeugen von SMGW-Zertifikatsrequests ausgelöst durch den GWA	Das SMGW **MUSS** ▸FA.DoSmgwPkiCertRequest für den GWA umsetzen. [REQ.WAN.Management.200]
Importieren von SMGW-WAN-Zertifikaten durch den GWA	Das SMGW **MUSS** ▸FA.DoImportSmgwPkiCerts für den GWA umsetzen. [REQ.WAN.Management.201]
Löschen von nicht benötigten SMGW-WAN-Zertifikaten durch den GWA	Das SMGW **MUSS** ▸FA.DoDeactivateSmgwPkiCerts für den GWA umsetzen. [REQ.WAN.Management.202]
Vorbereitung des Sicherheitsmodules durch den GWA	Das SMGW **MUSS** ▸FA.DoPrepareSecmod für den GWA umsetzen. [REQ.WAN.Management.196]
Bereitstellung von Schlüsselobjekt-Referenzen des Sicherheitsmodules und weiteren Zustandsinformationen	Das SMGW **MUSS** ▸FA.ReadSecmodState für den GWA umsetzen. [REQ.WAN.Management.197]
HAN	
Erzeugen eines neuen SMGW-HAN-Schlüsselpaares und selbstsignierten Zertifikates ausgelöst durch den GWA	Das SMGW **MUSS** ▸FA.DoCreateSelfsignedSmgwHanCert für den GWA umsetzen. [REQ.WAN.Management.220]
Nicht benötigtes Schlüsselpaar und selbstsigniertes TLS-Zertifikat des SMGW im HAN durch GWA deaktivieren	Das SMGW **MUSS** ▸FA.DoDeactivateSelfsignedSmgwHanCert für den GWA umsetzen. [REQ.WAN.Management.175]
LMN	
Erzeugen eines neuen SMGW-LMN-Schlüsselpaares und selbstsignierten Zertifikates ausgelöst durch den GWA	Das SMGW **MUSS** ▸FA.DoCreateSelfsignedSmgwLmnCert für den GWA umsetzen. [REQ.WAN.Management.210]
Nicht benötigtes Schlüsselpaar und selbstsigniertes TLS-Zertifikat des SMGW im LMN durch GWA deaktivieren	Das SMGW **MUSS** ▸FA.DoDeactivateSelfsignedSmgwLmnCert für den GWA umsetzen. [REQ.WAN.Management.172]

Tabelle 3.56 Übersicht der FA der Kategorie FAKAT.SmgwCertMgmt

ICS



ICS.FAKAT.SmgwCertMgmt.10

Der GWH **MUSS** im ICS angeben, ob das SMGW ▸Abschnitt 3.19.9 für die Rolle GWA umsetzt.

3.19.3 Datenstrukturen

Die Datenstruktur mit dem SMGW-Zertifikatssatz ist in ▸Abschnitt 3.22.42 beschrieben.

Die Datenstruktur mit dem RootCA-Zertifikatssatz ist in ▸Abschnitt 3.22.39 beschrieben.

Die Datenstruktur mit den CSR-Parametern ist in ▸Abschnitt 3.22.14 beschrieben.

Die Datenstruktur eines Zertifikats ist in ▸Abschnitt 3.22.48 beschrieben.

Die Datenstruktur zur Erzeugung eines Zertifikat/Schlüsselpaares ist in ▸Abschnitt 3.22.11 beschrieben.

3.19.4 FA.DoImportRootCaCert

3.19.4.1 Beschreibung

Importiert und aktiviert ein neues SM-PKI-Root-CA Zertifikat in das Sicherheitsmodul des SMGW, um den Vertrauensanker der SM-PKI zu aktualisieren.

Sofern ein ROOTCA-Link-Zertifikat (ROOTCA_LINK_CRT$_n$) übergeben wird, prüft das SMGW die zeitliche und inhaltliche Gültigkeit des Link-Zertifikates und validiert dieses Link-Zertifikat mit dem im SMGW vorliegenden öffentlichen Schlüssel des bisherigen ROOTCA_SIG_CRT$_n$ und validiert das als Aufrufparameter übergebene neue ROOTCA_SIG_CRT$_{n+1}$ mit dem übergebenen Link-Zertifikat.

Der GWA als Aufrufer des FA hat damit die Möglichkeit (und Verantwortung), den Übergang auf einen neuen (SM-PKI-)Vertrauensanker im SMGW im Falle eines nicht mit dem im SMGW gespeicherten RootCA-Zertifikates validierbaren Link-Zertifikat auch ohne Kontrolle des SMGW zu vollziehen.

Nachdem das SMGW die zeitliche und inhaltliche Gültigkeit des übermittelten neuen ROOTCA-Signatur-Zertifikates (ROOTCA_SIG_CRT$_{n+1}$) geprüft hat, persistiert das SMGW das ROOTCA_SIG_CRT$_{n+1}$ und den darin enthaltenen öffentlichen Schlüssel ROOTCA_SIG_PUB$_{n+1}$ im SM des SMGW.

Damit dieser FA ausgeführt werden kann, muss das Sicherheitsmodul des SMGW sich im AUTH-Zustand befinden, d.h. der GWA ist am SM authentifiziert, damit der Vertrauensanker und der zugehörige öffentliche Schlüssel in das Sicherheitsmodul importiert werden können.

Ein Aufrufparameter bestimmt das für den Schlüsselimport in das Sicherheitsmodul notwendige CV-Zertifikat. Das SMGW persistiert das RootCA-Zertifikat nur, wenn der Import des Public Keys erfolgreich war. Der GWA berechnet das CV-Zertifikat passend zum RootCA-Zertifikat.

Der GWA muss dazu am Sicherheitsmodul authentifiziert sein.

3.19.4.2 Auslöser



REQ.FA.DoImportRootCaCert.80

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.19.4.3 Anforderungen

- Das SMGW **SOLL** die Datenfelder gemäß ▸Tabelle 3.57 auf Plausibilität prüfen und im Fehlerfall den Import ablehnen. ▸ [BSI.17009.2] . [REQ.FA.DoImportRootCaCert.15]
- Das SMGW **MUSS** den Import ablehnen, wenn das Datenfeld ▸rootKeyCvCert nicht vorhanden ist. [REQ.FA.DoImportRootCaCert.70]
- Das SMGW **MUSS** das validierte ROOTCA_SIG_CRT$_{n+1}$ und den zugehörigen Schlüssel persistieren und für künftige Validierung von SM-PKI SubCA-Zertifikaten verwenden. ▸ [FNN.17009.0] ▸ [FNN.17009.1] [REQ.FA.DoImportRootCaCert.60] Sofern das vorherige Root-CA-Signaturzertifikat ROOTCA_SIG_CRT$_n$ noch nicht vom GWA gelöscht wurde, kann dies in der Übergangsphase bis alle SubCA-Zertifikate umgestellt sind, weiterhin für die Validierung verwendet werden.

Nr.	Bedingung	Datenfeld	Prüfung
1	Immer	▸rootCert im Aufrufparameter (ROOTCA_SIG_CRT$_{n+1}$)	Entspricht dem Zertifikatsprofil C(Root) gemäß [TR-03109-4].
2	Immer	▸rootCert im Aufrufparameter (ROOTCA_SIG_CRT$_{n+1}$)	Der *SubjectCN* entspricht [SM-PKI-CP] Anhang A oder Anhang C der Wirk-PKI oder Test-PKI.
3	Immer	▸rootCert im Aufrufparameter (ROOTCA_SIG_CRT$_{n+1}$)	Ist noch mindestens 30 Tage gültig.
4	Aufrufparameter ▸linkCert vorhanden.	Aufrufparameter ▸rootCert und ▸linkCert	Die Signatur des ▸rootCert im Aufrufparameter (ROOTCA_SIG_CRT$_{n+1}$) kann mit dem Schlüssel des ROOTCA_LINK_CRT validiert werden und die Signatur des ▸linkCert kann mit dem im SMGW persistierten Schlüssel des ROOTCA_SIG_CRT$_n$ validiert werden.
5	Immer	Aufrufparameter ▸rootKeyCvCert und ▸rootCert	Der öffentliche Schlüssel im Import-CV-Zertifikat ▸rootKeyCvCert entspricht dem öffentlichen Schlüssel des ▸rootCert

Tabelle 3.57 Plausibilitätsprüfungen

ICS



ICS.FA.DoImportRootCaCert.10

Der GWH **MUSS** im ICS deklarieren, welche Plausibilitätsprüfungen das SMGW gemäß ▸Tabelle 3.57 durchführt.

3.19.5 FA.DoDeactivateRootCaCert

3.19.5.1 Beschreibung

Ein im (Sicherheitsmodul des) SMGW gespeichertes RootCA-Zertifikat wird deaktiviert, so dass es künftig nicht mehr als Vertrauensanker für die Validierung von Zertifikaten verwendet werden kann.

Das zu deaktivierende X.509-Zertifikat wird über den Subject Key Identifier im Aufrufparameter identifiziert.

Der GWA muss dazu am Sicherheitsmodul authentifiziert sein.

3.19.5.2 Auslöser



REQ.FA.DoDeactivateRootCaCert.50

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.19.5.3 Anforderungen

- Das SMGW **MUSS** das Deaktivieren ablehnen, wenn der Aufrufparameter (Subject Key Identifier des ▸cert) keinem im SMGW bzw. Sicherheitsmodul persistierten Root-CA-Zertifikat entspricht. ▸ [FNN.17010.2] [REQ.FA.DoDeactivateRootCaCert.10]
- Das SMGW **MUSS** das Deaktivieren des RootCA-Zertifikates ablehnen, wenn noch ein damit ausgestelltes SubCA-Zertifikat zur Validierung eines im SMGW vorliegenden Endnutzerzertifikates benötigt wird. ▸ [FNN.17010.1] [REQ.FA.DoDeactivateRootCaCert.20]
- Das SMGW **MUSS** das RootCA-Zertifikat und den zugehörigen Public-Key ROOTCA_SIG_PUB so im Sicherheitsmodul deaktivieren, dass künftig ein neues RootCA-Zertifikat importiert werden kann ▸ ▸ [FNN.17010.0] [REQ.FA.DoDeactivateRootCaCert.30]
- Das SMGW **MUSS** das RootCA-Zertifikat so deaktivieren, dass das deaktivierte Zertifikat nicht mehr zur Validierung von SubCA-Zertifikaten verwendet werden kann. [REQ.FA.DoDeactivateRootCaCert.40]

3.19.6 FA.DoSmgwPkiCertRequest

3.19.6.1 Beschreibung

Das SMGW erzeugt auf Veranlassung durch den GWA (1) mit den Diensten des Sicherheitsmodules zunächst drei Schlüsselpaare (GW_WAN_TLS_PRV/PUB, GW_WAN_SIG_PRV/PUB, GW_WAN_ENC_PRV/PUB). Jedes Schlüsselpaar wird nun zur Erzeugung eines Zertifikats-*Einzelantrages* verwendet (2). Diese drei Einzelanträge werden in einem *Zertifikatsrequest-Paket* zusammengefasst und mit dem aktuellen vom SMGW verwendeten GW_WAN_SIG_PRV signiert (3) und als *Signiertes Zertifikatsrequest-Paket* an den Aufrufer übermittelt (4). An die Reihenfolge der *Einzelanträge* im *Zertifikatsrequest-Paket* werden keine Vorgaben gemacht.

Die Anforderungen an die Datenstrukturen *Einzelantrag* ("CertReqMsg"), *Zertifikatsrequest-Paket* ("CertReqMessages") und *Signiertes Zertifikatsrequest-Paket* ("SignedData") sind in [TR-03109-4] Anhang C beschrieben.

Die im Aufrufparameter (▸Parametersatz für CSR-Erzeugung) übergebenen Datenfelder bestimmen die Erzeugung der Schlüsselpaare und den Inhalt der *Einzelanträge*.

Dieser FA wird sowohl zum Erzeugen der initialen als auch für Folge-Anträge der SMGW-WAN-PKI-Zertifikate verwendet.

Der GWA muss zur Erzeugung der Schlüsselpaare am Sicherheitsmodul authentifiziert sein.

▸Abbildung 3.20 zeigt die Schlüssel- und Zertifikatsverarbeitung beim Erstellen neuer SMGW-PKI-Zertifikate im Zusammenspiel von SMGW, Sicherheitsmodul und GWA.

Die von der SubCA ausgestellten Zertifikate (GW_WAN_TLS_CRT, GW_WAN_SIG_CRT, GW_WAN_ENC_CRT) übermittelt der GWA mittels ▸FA.DoImportSmgwPkiCerts an das SMGW, das die Zertifikate importiert (5), sofern deren Public-Key dem zuvor in (2) erzeugten Public Keys entspricht. Nach erfolgreicher Aktualisierung der SMGW-Zertifikate und sobald sie nicht mehr vom SMGW benötigt werden deaktiviert der GWA mittels ▸FA.DoDeactivateSmgwPkiCerts die bisherigen SMGW-Zertifikate (6).

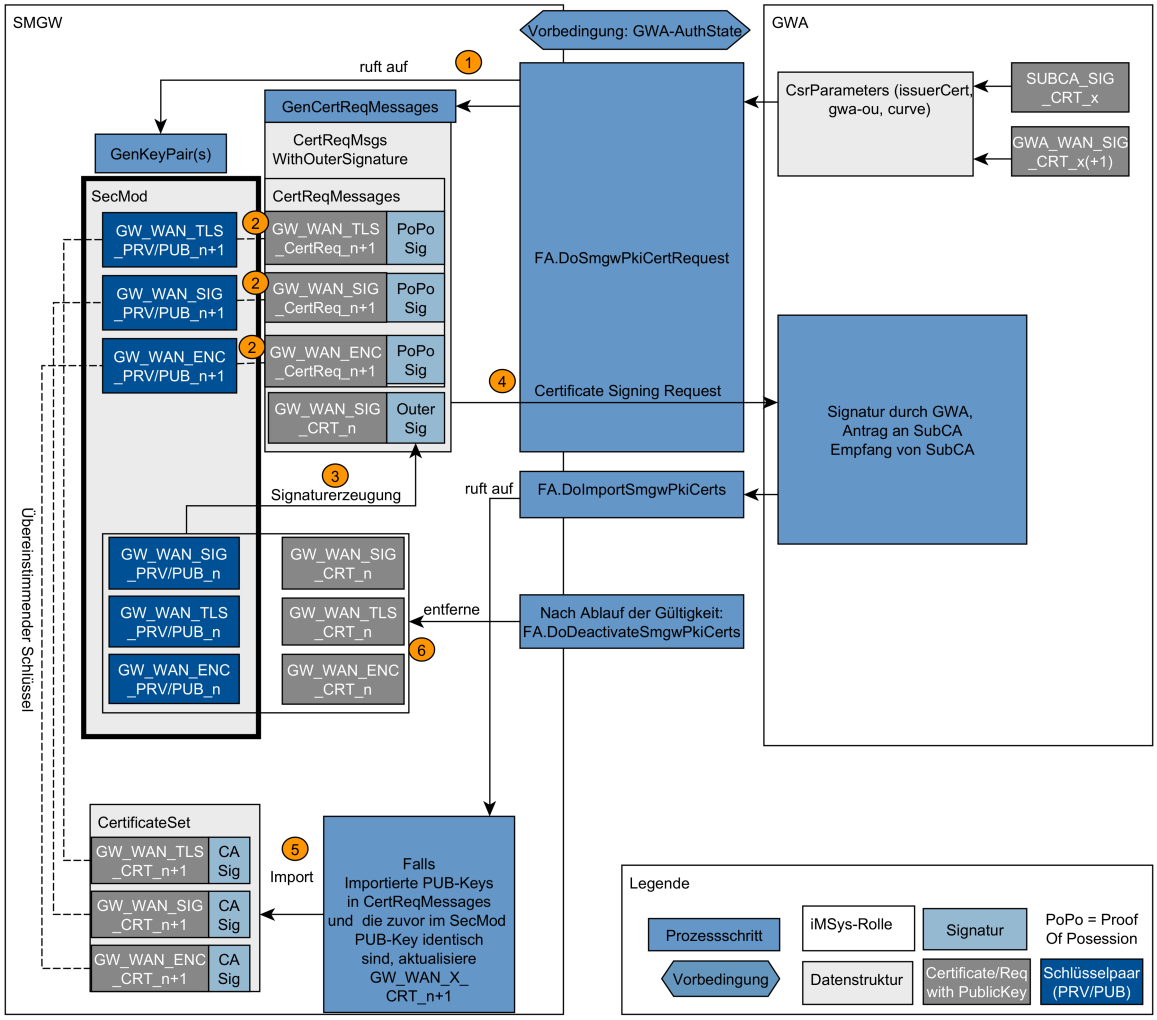


Abbildung 3.20. Schlüssel- und Zertifikatsverarbeitung beim Erstellen neuer SMGW-PKI-Zertifikate

3.19.6.2 Auslöser

REQ.FA.DoSmgwPkiCertRequest.60

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.19.6.3 Anforderungen

- Das SMGW **MUSS** die drei unterschiedlichen Schlüsselpaare GW_WAN_TLS_PRV/PUB, GW_WAN_SIG_PRV/PUB, GW_WAN_ENC_PRV/PUB mit den im Aufrufparameter ▸namedCurveId angegebenen Kurvenparametern erzeugen und persistieren, ohne die aktiven Schlüsselpaare zu überschreiben. ▸ [FNN.17003.2] [REQ.FA.DoSmgwPkiCertRequest.10]
- Das SMGW **MUSS** die "certTemplate.extensions" der jeweiligen "CertReqMsg" gemäß den Zertifikatsprofilen für C_{TLS}(SMGW), C_{Enc}(SMGW) und C_{Sig}(SMGW) in [TR-03109-4] Anhang A.2 mit den zuvor erzeugten

öffentlichen Schlüsseln erstellen und mit dem jeweiligen zugehörigen privaten Schlüssel signieren (Proof of Possession). [REQ.FA.DoSmgwPkiCertRequest.15] [15]

- Das SMGW **MUSS** die "SubjectKeyIdentifier" Extension nach [RFC5280] Kapitel 4.2.1.2 Methode 1 für den SubjectPublicKey jedes der drei "CertReqMsg" berechnen und setzen. [REQ.FA.DoSmgwPkiCertRequest.16] [16]
- Das SMGW **MUSS** das Attribut "OU" (Organizational Unit) des SubjectDN der "CertReqMsg" folgendermaßen setzen: Sofern das Datenfeld ▸ou des Aufrufparameters vorhanden ist und [SM-PKI-CP] Anhang A für die Funktion "GWA" entspricht, wird der Inhalt des Datenfeldes verwendet. Anderenfalls wird der Inhalt des SubjectDN Attributes "CN" (CommonName) aus dem aktuellen im SMGW gespeicherten GWA-Zertifikat (GWA_WAN_TLS_CRT) verwendet. [REQ.FA.DoSmgwPkiCertRequest.20]
- Das SMGW **MUSS** den "AuthorityKeyIdentifier" der drei "CertReqMsg" folgendermaßen setzen: Der Inhalt der Extension "AuthorityKeyIdentifier" des im Aufrufparameter ▸issuerCert übergebenen Issuer-Zertifikates. [REQ.FA.DoSmgwPkiCertRequest.30]
- Das SMGW **MUSS** das Attribut "O" (Organisation) des SubjectDN der drei "CertReqMsg" folgendermaßen setzen: SubjectDN Attribut "O" des aktuellen im SMGW verwendeten GW_WAN_TLS_CRT. [REQ.FA.DoSmgwPkiCertRequest.40]
- Das SMGW **MUSS** in jeder der drei "CertReqMsg" im Datenfeld "certTemplate.subject" den SubjectCN identisch mit dem Inhalt des SubjectCN des aktuellen GW_WAN_TLS_CRT setzen. [REQ.FA.DoSmgwPkiCertRequest.42]
- Das SMGW **MUSS** in jeder der drei "CertReqMsg" im Datenfeld "certTemplate.subject" (Attribut SERIALNUMBER) die Sequenznummer identisch und um "1" erhöht gegenüber der Sequenznummer im aktuellen GW_WAN_TLS_CRT wählen. [REQ.FA.DoSmgwPkiCertRequest.44]
- Das SMGW **MUSS** die Datenstruktur "SignedData (CertReqMessages)" gemäß [TR-03109-4] Anhang C erzeugen, mit dem privaten Schlüssel zum aktuellen GW_WAN_SIG_CRT signieren und als Rückgabeparameter des FA-Aufrufs übermitteln. ▸ [FNN.17003.0] ▸ [FNN.17003.1] [REQ.FA.DoSmgwPkiCertRequest.50]

3.19.7 FA.DoImportSmgwPkiCerts

3.19.7.1 Beschreibung

Das SMGW prüft und persistiert die als Aufrufparameter übergebenen TLS-, Signatur- und Verschlüsselungszertifikate für das SMGW aus der SM-PKI.

Sofern die im Aufrufparameter (Siehe ▸SMGW-Zertifikatssatz) übergebenen Zertifikate GW_WAN_TLS_CRT, GW_WAN_SIG_CRT, GW_WAN_ENC_CRT den zuvor mit ▸FA.DoSmgwPkiCertRequest erstellten Schlüsseln zugeordnet werden können, speichert das SMGW die als Aufrufparameter übergebenen Zertifikate zur künftigen Verwendung durch das SMGW.

Alle Zertifikate des Zertifikatstripels werden immer gemeinsam importiert. Schlägt der Import oder die Aktivierung eines Zertifikats fehl, wird keines der Zertifikate des Zertifikatstripels aktiviert.

Nach dem erfolgreichen Ausführen dieses FA verwendet das SMGW die Zertifikate unmittelbar: Vom SMGW erzeugte Inhaltsdatennachrichten werden mit dem $GW_WAN_SIG_CRT_n$ signiert, (vom GWA) empfangene Inhaltsdaten werden je nach verwendetem Schlüssel mit $GW_WAN_ENC_CRT_n$ oder $GW_WAN_ENC_CRT_{n-1}$ entschlüsselt und bei neu aufgebauten TLS-Verbindungen im WAN authentifiziert sich das SMGW mit dem $GW_WAN_TLS_CRT_n$. Aus diesem Grund ist ein kontrollierter Betriebsprozess zum Wechsel der SMGW Zertifikate im Zusammenspiel mit den EMT/GWA Backendsystemen notwendig (Siehe [TR-03109-1-VI]). Solange der private Schlüssel zum $GW_WAN_ENC_CRT_{n-1}$ noch im (Sicherheitsmodul des) SMGW aktiv ist, kann er für die Entschlüsselung von Inhaltsdatennachrichten verwendet werden. Solange der private Schlüssel zum

[15] Es wird klargestellt: Die Übermittlung der Extension "Subject Alternate Name" in "certTemplate.extensions" ist nicht erforderlich.

[16] Nach [TR-03109-4] Kapitel C.2.1 ist die SubjectKeyIdentifier Extension optional. Dies bedeutet, dass die CA den SKI berechnet. Das SMGW hat keine Informationen nach welcher Methode der SKI berechnet wurde. Mit dieser Anforderung unterliegt die Kontrolle der Berechnungsmethode dem SMGW.

bisherigen GW_WAN_TLS_CRT$_{n-1}$ noch im (Sicherheitsmodul des) SMGW aktiv ist, können Kommunikationspartner mit einer "Hello-Extension" beim TLS-Verbindungsaufbau bestimmen, dass sich das SMGW mit dem GW_WAN_TLS_CRT$_{n-1}$ authentifiziert.

Solange das bisherige GW_WAN_SIG_CRT$_{n-1}$ noch im SMGW persistiert ist, kann es dem Anschlussnutzer für die Validierung von archivierten signierten Messwerten bereitgestellt werden.

Die bisherigen Schlüssel und Zertifikate GW_WAN_TLS_CRT$_{n-1}$, GW_WAN_SIG_CRT$_{n-1}$, GW_WAN_ENC_CRT$_{n-1}$ können anschließend durch ▸FA.DoDeactivateSmgwPkiCerts deaktiviert werden.

Da die öffentlichen Schlüssel zu den Zertifikaten bereits im Sicherheitsmodul vorliegen, ist eine Authentifizierung des GWA am Sicherheitsmodul nicht notwendig.

3.19.7.2 Auslöser



REQ.FA.DoImportSmgwPkiCerts.50

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.19.7.3 Anforderungen

- (▸ICS.FA.DoImportSmgwPkiCerts.10) Das SMGW **SOLL** die Zertifikate im Aufrufparameter gemäß ▸Tabelle 3.58 validieren und den Import bei mindestens einer nicht bestandenen Prüfung ablehnen.▸ [FNN.17002.1] [REQ.FA.DoImportSmgwPkiCerts.20]
- Das SMGW **MUSS** die Zertifikate des Zertifikatssatzes (GW_WAN_TLS_CRT, GW_WAN_SIG_CRT, GW_WAN_ENC_CRT und - falls im Aufrufparameter übergeben - SubCA-Zertifikat) persistieren und für die künftige Kommunikation verwenden. ▸ [FNN.17002.2] ▸ [FNN.17002.0] [REQ.FA.DoImportSmgwPkiCerts.30]
- (▸ICS.HAN.SicherungKommunikation.10) Das SMGW **MUSS**+ das GW_WAN_TLS_CRT für die künftige Authentisierung als GW_HAN_TLS_CRT im HAN anbieten. [REQ.FA.DoImportSmgwPkiCerts.60]

Nr.	Bedingung	Datenfeld	Prüfung
1	Immer	▸tlsCert, ▸sigCert, ▸encCert	Alle Datenfelder sind vorhanden und DER-Co-diert gemäß [X.690].
2	Immer	▸tlsCert, ▸sigCert, ▸encCert	Die *SubjectDN* der Zertifikate sind identisch.
3	Immer	▸tlsCert, ▸sigCert, ▸encCert	Die *IssuerDN* der Zertifikate sind identisch.
4	Immer	▸tlsCert, ▸sigCert, ▸encCert	Das Datenfeld "valid.notAfter" aller Zertifikate liegt bzgl. der Systemzeit noch mindestens 30 Tage in der Zukunft (d.h. die Zertifikate sind noch mindestens 30 Tage gültig).
5	Immer	▸tlsCert, ▸sigCert, ▸encCert	Das Datenfeld "valid.notBefore" aller Zertifikate liegt bzgl. der Systemzeit in der Vergangenheit.
6	Immer	▸tlsCert, ▸sigCert, ▸encCert	Alle Zertifikate enthalten im *SubjectCN* die Funktion "smgw"
7	▸caCert im Aufrufparameter vorhanden	▸tlsCert, ▸sigCert, ▸encCert, ▸caCert	Der *SubjectDN* des ▸caCert entspricht dem IssuerDN der zu importierenden SMGW-Zertifikate.
8	Immer	▸tlsCert	Die KeyUsage-Extension des TLS-Zertifikates erlaubt "DigitalSignature" und das TLS-Zertifikat besitzt eine ExtendedKeyUsage-Extension.
9	Immer	▸sigCert	Die KeyUsage-Extension des Signatur-Zertifikates erlaubt "DigitalSignature" und das Signatur-Zertifikat besitzt keine ExtendedKeyUsage-Extension.
10	Immer	▸encCert	Die KeyUsage-Extension des Verschlüsselungs-Zertifikates erlaubt "KeyEncipherment" und "KeyAgreement".

Nr.	Bedingung	Datenfeld	Prüfung
11	▸caCert im Aufrufparameter vorhanden	▸caCert	Die KeyUsage-Extension des CA-Zertifikates erlaubt "DigitalSignature"

Tabelle 3.58 Plausibilitätsprüfungen

ICS



ICS.FA.DoImportSmgwPkiCerts.10

Der GWH **MUSS** im ICS deklarieren, welche Plausibilitätsprüfungen das SMGW gemäß ▸Tabelle 3.58 durchführt.

3.19.8 FA.DoDeactivateSmgwPkiCerts

3.19.8.1 Beschreibung

Nach Ausführen dieses FA können die Zertifikate und Schlüsselpaare GW_WAN_TLS_PUB/PRV/CRT_{n-1}, GW_WAN_ENC_PUB/PRV/CRT_{n-1} und GW_WAN_SIG_PUB/PRV/CRT_{n-1} nicht mehr zur Kommunikation, Verschlüsselung, Signatur verwendet werden.

Der GWA muss dazu am Sicherheitsmodul authentifiziert sein.

3.19.8.2 Auslöser



REQ.FA.DoDeactivateSmgwPkiCerts.30

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.19.8.3 Anforderungen

- Das SMGW **MUSS** die Deaktivierung der Schlüsselpaare und Zertifikate ablehnen, wenn das GW_WAN_TLS_CRT_{n-1} für die TLS-Authentifizierung an einer der Schnittstellen des SMGW verwendet wird. ▸[FNN.17006.1] [REQ.FA.DoDeactivateSmgwPkiCerts.10] Ein Schlüssel/Zertifikat wird "verwendet", wenn die einzig verbliebene TLS-Authentifizierungsmöglichkeit des SMGW an der jeweiligen Schnittstelle auf diesem Zertifikat basiert.
- Das SMGW **MUSS** die Schlüsselpaare und Zertifikate GW_WAN_TLS_PUB/PRV/CRT_{n-1}, GW_WAN_ENC_PUB/PRV/CRT_{n-1} und GW_WAN_SIG_PUB/PRV/CRT_{n-1} gemeinsam deaktivieren. Kann ein Schlüsselpaar oder Zertifikat nicht deaktiviert werden, so werden alle nicht deaktiviert bzw. Deaktivierungen zurückgenommen. [REQ.FA.DoDeactivateSmgwPkiCerts.12]
- Das SMGW **MUSS** das SMGW-Zertifikatstripel mit dem ältesten Ausstellungsdatum (validity.notBefore) und die zugehörigen Schlüssel im Sicherheitsmodul so deaktivieren, so dass ein folgender Aufruf von ▸FA.DoSmgwPkiCertRequest neue Schlüsselpaare und Zertifikate erzeugen kann und die deaktivieren Zertifikate nicht mehr für die Kommunikation verwendet werden können. ▸[FNN.17006.0] ▸[BSI.17006.92] [REQ.FA.DoDeactivateSmgwPkiCerts.20] Sofern das zugehörige SubCA-Zertifikat nicht mehr benötigt wird, kann es gelöscht werden.

3.19.8.4 Implementierungshinweise

Die Funktionalität ist Ausfallsicher zu implementieren. D.h. zu keiner Zeit darf ein Zustand eintreten, bei dem kein gültiges SMGW-Schlüsselmaterial mehr im SMGW nutzbar ist.

Sofern der Vorgang nicht atomar abgeschlossen werden kann (z.B. weil nicht alle zusammengehörigen Schlüssel und Zertifikate gelöscht werden konnte) oder Vorbedingungen nicht eingehalten wurden, soll durch erneuten Aufruf des FAs die Möglichkeit bestehen, das Schlüssel- und Zertifikatsmaterial zu deaktivieren.

3.19.9 FA.ReadCertificate

3.19.9.1 Beschreibung

Das über einen Aufrufparameter (Siehe ▸Tabelle 3.59) selektierte, im SMGW persistierte Zertifikat wird an den Aufrufer exportiert. Zur Transparenz für die Anwender des SMGW muss das SMGW Auskunft über die aktiven für die Zertifikatsprüfungen verwendeten Zertifikate geben. Insbesondere alle (im Sicherheitsmodul gespeicherten) RootCA-Zertifikate müssen auslesbar sein.

Die Zertifikate der Kommunikationspartner des SMGW sind über deren jeweilige WAN-, HAN-, LMN-Kommunikationsprofile auslesbar. GWA-Zertifikatssätze sind sowohl über diesen FA als auch über die GWA-Kommunikationsprofile auslesbar.

Typ	Beschreibung
ROOTCA_SIG_n	Zertifikate von RootCAs (n>=1)
GWA_WAN_TLS/SIG/ENC_CRT	Das aktuelle GWA-TLS/SIG/ENC-Zertifikat (zur Domäne "gwa")
GWA_WAN_TLS/SIG/ENC_CRT_PREV	Das Alternatives/Vorheriges im SMGW gespeicherte GWA-TLS/SIG/ENC-Zertifikat (zur Domäne "gwapre")
CA_SIG_CRT_n	Zertifikate von SubCAs (n>=1)
GW_WAN_TLS/SIG/ENC_CRT	Das primäre SMGW-TLS/SIG/ENC-WAN-Zertifikat
GW_WAN_TLS/SIG/ENC_CRT_PREV	Vorheriges SMGW-TLS/SIG/ENC-Zertifikat
GW_LMN_TLS_CRT	Das aktuelle vom SMGW an der LMN-Schnittstelle verwendete Zertifikat
GW_LMN_TLS_CRT_PREV	Das vorherige vom SMGW an der LMN-Schnittstelle verwendete Zertifikat
GW_HAN_TLS_CRT	Das aktuelle vom SMGW an der HAN-Schnittstelle verwendete Zertifikat
GW_HAN_TLS_CRT_PREV	Das vorherige vom SMGW an der HAN-Schnittstelle verwendete Zertifikat

Tabelle 3.59 Filter zur Auflistung von Zertifikaten

3.19.9.2 Auslöser



REQ.FA.ReadCertificate.30

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Empfang einer Anfrage über ▸HKS.WS1.

3.19.9.3 Anforderungen

Sofern das im Aufrufparameter gemäß ▸Tabelle 3.59 selektierte X.509-Zertifikat im SMGW persistiert und aktiviert ist, **SOLL** das SMGW das Zertifikat gemäß ▸Abschnitt 3.22.48 an den Aufrufer exportieren (▸ICS.FA.ReadCertificate.20. [REQ.FA.ReadCertificate.20]

ICS



ICS.FA.ReadCertificate.20

Der GWH **MUSS** im ICS deklarieren, welche Zertifikate ausgelesen werden können.

Das PREV-Zertifikat ("Previous"-Zertifikat) ist von zwei Zertifikaten gleichen Typs das ältere. Ohne "PREV" wird das aktuelle (jüngere) Zertifikat eines Typs identifiziert.

3.19.10 FA.DoCreateSelfsignedSmgwHanCert

3.19.10.1 Beschreibung

Das SMGW erzeugt ein neues GW_HAN_TLS_PRV$_{n+1}$/PUB$_{n+1}$ Schlüsselpaar und GW_HAN_TLS_CRT$_{n+1}$, ohne das bisherige GW_HAN_TLS_PRV$_n$/PUB$_n$ Schlüsselpaar und GW_HAN_TLS_CRT$_n$ zu überschreiben.

Über Aufrufparameter können Schlüssellänge (Kurvenparameter) und Zertifikatsfelder bestimmt werden.

Der GWA muss am Sicherheitsmodul authentifiziert sein.

Dieses Zertifikat wird künftig als TLS-Server- bzw. TLS-Client-Zertifikat des SMGW verwendet, damit sich das SMGW damit gegenüber den HAN-Teilnehmern authentifizieren kann. Ausgewählt durch die vom HAN-Teilnehmer initiierte Verbindung[17] kann das SMGW eines der aktiven TLS-Server Zertifikate präsentieren (GW_WAN_TLS_CRT (SM-PKI), GW_HAN_TLS_CRT$_{n-1}$, GW_HAN_TLS_CRT$_n$), die der HAN-Teilnehmer mit seinem Vertrauensanker validieren kann.

3.19.10.2 Auslöser



REQ.FA.DoCreateSelfsignedSmgwHanCert.40

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.19.10.3 Anforderungen

- Sofern die im Aufrufparameter ▸namedCurveId übergebenen kryptografischen Vorgaben für die Erzeugung der Schlüssel und Zertifikatsinhalte nicht unterstützt werden, **MUSS** das SMGW die Erzeugung des Schlüsselpaares/Zertifikates ablehnen. ▸ [BSI.17011.92] [REQ.FA.DoCreateSelfsignedSmgwHanCert.20]
- Das SMGW **MUSS** das Schlüsselpaar GW_HAN_TLS_PRV/PUB$_{n+1}$ mit den im Aufrufparameter ▸namedCurveId angegebenen Kurvenparametern gemäß [TR-03109-3] erzeugen und persistieren, ohne das aktive Schlüsselpaar GW_HAN_TLS_PRV/PUB$_n$ zu verändern. ▸ [FNN.17011.1] [REQ.FA.DoCreateSelfsignedSmgwHanCert.10]



REQ.FA.DoCreateSelfsignedSmgwHanCert.30

Das SMGW **MUSS** ein GW_HAN_TLS_CRT$_{n+1}$ erzeugen, um

- den frisch erzeugten öffentlichen Schlüssel GW_HAN_TLS_PUB als *subjectPublicKey* verwenden,
- das Zertifikat nach den Vorgaben von [DS] HAN-Zertifikatprofile für das SMGW CT_Selfsigned (Typ A) erzeugen,
- mit dem privaten Schlüssel GW_HAN_TLS_PRV signieren,
- im SMGW persistieren und künftig für die TLS-Authentifizierung im HAN verwenden,
- gemäß ▸Abschnitt 3.22.48 an den Aufrufer übermitteln.

▸ [BSI.17011.92] ▸ [FNN.17011.0]

ICS



ICS.ZertifikateHAN.Allgemein.30

Der GWH **MUSS** im ICS deklarieren, welche Laufzeit (aufgerundet in Monaten) die von der Implementierung erstellten GW_HAN_TLS_CRT-Zertifikate vom Typ CT_Selfsigned besitzen (0: Wenn die Laufzeit nicht begrenzt ist).

3.19.11 FA.DoDeactivateSelfsignedSmgwHanCert

3.19.11.1 Beschreibung

Das nicht mehr für die Kommunikation benötigte selbstsignierte GW_HAN_TLS_CRT$_n$ des SMGW und das zugehörige Schlüsselpaar kann künftig nicht mehr für die Authentifizierung des SMGW verwendet werden.

Das Deaktivieren ist erst dann möglich, nachdem alle über das HAN kommunikativ angebundenen Geräte das aktuelle GW_HAN_TLS_CRT$_n$ zur Authentifizierung des SMGW verwenden können.

Der GWA muss dazu am Sicherheitsmodul authentifiziert sein.

[17] Z.B. TCP-Port oder TLS-Client-Hello Extension

3.19.11.2 Auslöser



REQ.FA.DoDeactivateSelfsignedSmgwHanCert.40

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.19.11.3 Anforderungen

- Das SMGW **MUSS** das Deaktivieren ablehnen, wenn im SMGW nicht mehr als ein GW_HAN_TLS_CRT und Schlüsselpaar aktiviert ist. ▸ [FNN.17013.1] [REQ.FA.DoDeactivateSelfsignedSmgwHanCert.10]
- Das SMGW **MUSS** das $GW_HAN_TLS_CRT_{n-1}$ so deaktivieren, dass es künftig nicht mehr zur Authentifizierung des SMGW im TLS-Handshake verwendet werden kann. ▸ [FNN.17013.0] [REQ.FA.DoDeactivateSelfsignedSmgwHanCert.30]

3.19.12 FA.DoCreateSelfsignedSmgwLmnCert

3.19.12.1 Beschreibung

Das SMGW erzeugt ein neues $GW_LMN_TLS_PRV_{n+1}/PUB_{n+1}$ Schlüsselpaar und $GW_LMN_TLS_CRT_{n+1}$ ohne das bisherige $GW_LMN_TLS_PRV_n/PUB_n$ Schlüsselpaar und $GW_LMN_TLS_CRT_n$ zu überschreiben.

Dieses Zertifikat wird künftig als TLS-Server- bzw. TLS-Client-Zertifikat des SMGW verwendet, um sich damit gegenüber den LMN-Teilnehmern authentifizieren zu können.

Über Aufrufparameter können Schlüssellänge (Kurvenparameter) und Zertifikatsfelder bestimmt werden.

Der GWA muss dazu am Sicherheitsmodul authentifiziert sein.

3.19.12.2 Auslöser



REQ.FA.DoCreateSelfsignedSmgwLmnCert.40

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.19.12.3 Anforderungen

- Sofern die im Aufrufparameter ▸namedCurveId übergebenen kryptografischen Vorgaben für die Erzeugung der Schlüssel und Zertifikatsinhalte nicht unterstützt werden, **MUSS** das SMGW die Erzeugung des Schlüsselpaares/Zertifikates ablehnen. ▸ [BSI.17014.93] [REQ.FA.DoCreateSelfsignedSmgwLmnCert.20]
- Das SMGW **MUSS** das Schlüsselpaar $GW_LMN_TLS_PRV/PUB_{n+1}$ mit den im Aufrufparameter ▸namedCurveId angegebenen Kurvenparametern gemäß [TR-03109-3] erzeugen und persistieren ohne das aktive Schlüsselpaar $GW_LMN_TLS_PRV/PUB_n$ zu verändern. ▸ [FNN.17014.1] [REQ.FA.DoCreateSelfsignedSmgwLmnCert.10]



REQ.FA.DoCreateSelfsignedSmgwLmnCert.30

Das SMGW **MUSS** ein $GW_LMN_TLS_CRT_{n+1}$ erzeugen, und

- den frisch erzeugten öffentlichen Schlüssel GW_LMN_TLS_PUB als *subjectPublicKey* verwenden,
- das Zertifikat nach den Vorgaben von [DS] LMN-Zertifikatprofile für das SMGW CT_Selfsigned (Typ A) erzeugen,
- mit dem privaten Schlüssel GW_LMN_TLS_PRV signieren,
- im SMGW persistieren und künftig für die TLS-Authentisierung des SMGW im LMN verwenden,
- das Zertifikat gemäß ▸X.509-Zertifikat (Certificate) an den Aufrufer übermitteln.

▸ [FNN.17014.0]

3.19.13 FA.DoDeactivateSelfsignedSmgwLmnCert

3.19.13.1 Beschreibung

Das nicht mehr für die Kommunikation benötigte, selbstsignierte GW_LMN_TLS_CRT$_{n-1}$ des SMGW und das zugehörige Schlüsselpaar kann künftig nicht mehr für die Authentifizierung des SMGW verwendet werden.

Das Deaktivieren ist erst dann möglich, nachdem alle über das LMN kommunikativ angebundenen Messeinrichtungen das aktuelle GW_LMN_TLS_CRT$_n$ zur Authentifizierung des SMGW verwenden können.

Der GWA muss dazu am Sicherheitsmodul authentifiziert sein.

3.19.13.2 Auslöser



REQ.FA.DoDeactivateSelfsignedSmgwLmnCert.40

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.19.13.3 Anforderungen

- Das SMGW **MUSS** das Deaktivieren ablehnen, wenn im SMGW nicht mehr als ein GW_LMN_TLS_CRT und Schlüsselpaar aktiviert ist. ▸ [FNN.17015.1] [REQ.FA.DoDeactivateSelfsignedSmgwLmnCert.10]
- Das SMGW **MUSS** das Deaktivieren ablehnen, wenn noch Geräte kommunikativ an das SMGW angebunden sind, die das GW_LMN_TLS_CRT$_{n-1}$ zur Authentisierung des SMGW benötigen. ▸ [BSI.17015.92] [REQ.FA.DoDeactivateSelfsignedSmgwLmnCert.20]
- Das SMGW **MUSS** das GW_LMN_TLS_CRT$_{n-1}$ so deaktivieren, dass es künftig nicht mehr zur Authentifizierung des SMGW im TLS-Handshake verwendet werden kann. ▸ [BSI.17015.93] ▸ [FNN.17015.0] [REQ.FA.DoDeactivateSelfsignedSmgwLmnCert.30]

3.19.14 FA.DoPrepareSecmod

3.19.14.1 Beschreibung

Das Sicherheitsmodul im SMGW wird für den Wirkbetrieb des SMGW vorbereitet, sofern dies noch nicht erfolgt ist.

Das Sicherheitsmodul ist initial mit einem Satz Schlüsselobjekte für GW_WAN_TLS_PUB/PRV, GW_WAN_SIG_PUB/PRV, GW_WAN_ENC_PUB/PRV, GW_LMN_TLS_PUB/PRV, GW_HAN_TLS_PUB/PRV ausgestattet. Durch Aufruf dieses FA wird unter Kontrolle des GWA jeweils ein zweites Schlüsselobjekt im Sicherheitsmodul angelegt, um künftig Ausfallsichere Zertifikats- und Schlüssel-Wechselprozesse der SMGW-Zertifikate zu unterstützen.

Dieser FA wird einmalig bei oder nach Personalisierung durch den GWA aufgerufen. Der GWA muss dazu am Sicherheitsmodul authentifiziert sein.

Sofern aufgrund eines Fehlers nicht alle Schlüsselobjekte gleichzeitig angelegt werden können, kann der FA nach Beseitigung der Fehlerursache erneut aufgerufen werden und vorher angelegte Objekte werden überschrieben oder übergangen.

3.19.14.2 Auslöser



REQ.FA.DoPrepareSecmod.20

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.19.14.3 Anforderungen

Das SMGW **MUSS** das Sicherheitsmodul so vorbereiten, dass künftig neue Schlüsselpaare und Zertifikate GW_WAN_TLS_PRV/PUB/CRT$_{n+1}$, GW_WAN_SIG_PRV/PUB/CRT$_{n+1}$, GW_WAN_ENC_PRV/PUB/CRT$_{n+1}$, GW_HAN_TLS_PRV/PUB/CRT$_{n+1}$, GW_LMN_TLS_PRV/PUB/CRT$_{n+1}$ vom SMGW erzeugt werden können,

ohne die jeweils aktiven Schlüssel und Zertifikate GW_(WAN/HAN/LMN)_(TLS/SIG/ENC)_(PRV/PUB/CRT)$_n$ zu überschreiben oder zuvor zu deaktivieren. ▸ [FNN.17025.1] ▸ [FNN.17025.0] [REQ.FA.DoPrepareSecmod.10]

3.19.15 FA.DoPrepareImportRootCaKey

3.19.15.1 Beschreibung

Dieser FA übermittelt dem Aufrufer den für die Erzeugung des Root-CA-Importzertifikates erforderliche Schlüsselreferenz zum nachfolgenden Import des Root-CA-Zertifikates (siehe ▸FA.DoImportGwaKeys).

3.19.15.2 Auslöser

REQ.FA.DoPrepareImportRootCaKey.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.19.15.3 Anforderungen

Das SMGW **MUSS** ein neues Schlüsselobjekt für den Import eines Root-CA-Public-Keys im Sicherheitsmodul erzeugen und dem Aufrufer die Schlüsselreferenz des für den Import des Root-CA-Schlüssels vorgesehen Schüsselobjektes mittels ▸rootCaKeyRef übermitteln. [REQ.FA.DoPrepareImportRootCaKey.20]

3.19.16 FA.ReadSecmodState

3.19.16.1 Beschreibung

Dieser FA stellt dem GWA die folgenden Informationen des Sicherheitsmoduls gemäß ▸Abschnitt 3.22.40 bereit:

- Die Schlüsselobjektreferenzen der in das Sicherheitsmodul importierten Schlüssel und deren Public-Keys (Für GWA- und RootCA-Zertifikate)
- Die im Sicherheitsmodul gespeicherten RootCA-Zertifikate

3.19.16.2 Auslöser

REQ.FA.ReadSecmodState.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.19.16.3 Anforderungen

Das SMGW **MUSS** dem Aufrufer die im Sicherheitsmodul gespeicherten RootCA-Zertifikate und Schlüsselobjektreferenzen und weitere Zustandsinformationen gemäß ▸Sicherheitsmodulzustand übermitteln. [REQ.FA.ReadSecmodState.20]

3.20 Firmware Download und Update (FAKAT.SmgwFwUpdate)

3.20.1 Übersicht

Die Anwendungsfälle dieser Kategorie beschreiben die Funktionalität zum Download und Aktualisierung von Firmware.

Die Funktionalität dieser FA-Kategorie wird neben der Durchführung von Updates des SMGW auch für die Bereitstellung von Dateien (beispielsweise Firmware-Updates) für Messeinrichtungen verwendet (siehe ▸FAKAT.MtrServices).

Der GWA stellt über einen Dateiserver die Firmware-Datei für den Download durch die SMGWs bereit und löst den Firmware-Update Anwendungsfall mit der für das jeweilige SMGW bzw. die Messeinrichtung passenden Download-URL aus.

Der Prozess wird über das FirmwareUpdateProfil gesteuert, das für jede Datei-Installation vom GWA konfiguriert wird.

Zum konfigurierten Zeitpunkt beginnt das SMGW den Download. Nach erfolgreichem Download und erreichtem Installationszeitpunkt beginnt die Installation im SMGW bzw. in der Messeinrichtung.

Bei der Installation im SMGW beginnt das SMGW die Validierung der Integrität und Herkunft der Firmware vom GWH. Nach erfolgreicher Validierung installiert und aktiviert das SMGW die Firmware. Ein Rückfall auf die vorherige Firmware ist nicht vorgesehen.

Bei der Installation in der Messeinrichtung beginnt das SMGW die Übertragung und Installation der Firmware in die Messeinrichtung. Es ist Aufgabe der Messeinrichtung, die Integrität und Herkunft der Firmware vom Messgerätehersteller zu validieren.

Der Download kann durch den GWA abgebrochen und neu gestartet werden. Das SMGW bereinigt in diesem Fall die Dateifragmente.

3.20.2 Übersicht der FA

Aufgabe	Umsetzung
Firmware-Update Konfiguration importieren und Download starten	Das SMGW **MUSS** ▸FA.UpdateFwUpdateConfig für den GWA umsetzen. [REQ.FAKAT.SmgwOperation.60]
Firmware-Update Download abbrechen	Das SMGW **SOLL** ▸FA.DeleteFwUpdateConfig für den GWA umsetzen. [REQ.FAKAT.FwDownload.30]
Firmware-Update Konfiguration auslesen	Das SMGW **MUSS** ▸FA.ReadFwUpdateConfig für den GWA umsetzen. [REQ.FAKAT.FwDownload.40]
Firmware-Download vom GWA für SMGW starten	Das SMGW **MUSS** ▸FA.DoFwDownload vom GWA für das SMGW umsetzen. [REQ.WAN.ZugriffAufGwaDienste.20]
Firmware-Download vom GWA für angebundene Komponente starten	(▸ICS.FAKAT.ValProcBilling.20) Das SMGW **MUSS+** ▸FA.DoFwDownload vom GWA für eine registrierende Messeinrichtung umsetzen. [REQ.FAKAT.FwDownload.50]
Firmware-Update in SMGW oder angebundene Komponente aktivieren	Das SMGW **SOLL** ▸FA.DoFwActivation für den GWA umsetzen. [REQ.WAN.Management.250]

Tabelle 3.60 Übersicht der FA der Kategorie FAKAT.SmgwFwUpdate

ICS



ICS.FAKAT.FwDownload.30

Der GWH **MUSS** im ICS deklarieren, ob das SMGW den ▸FA.DeleteFwUpdateConfig für den GWA umsetzt.

3.20.3 Datenstrukturen der FA-Kategorie

Das Firmwareupdateprofil ist in ▸Abschnitt 3.22.18 beschrieben.

3.20.4 FA.DoFwDownload

3.20.4.1 Beschreibung

Das SMGW nutzt einen Dienst des GWA, um eine neue Firmware- oder Parameter-Datei für das SMGW oder eine Messeinrichtung zu laden. Der Aufrufparameter identifiziert das Firmware-Update-Profil.

Dazu fordert das SMGW solange Teile der Datei an, bis die Datei vollständig im SMGW vorliegt oder eine zeitliche Grenze überschritten wird.

Während des Datei-Downloads sind die Dienste des SMGW uneingeschränkt verfügbar.

3.20.4.2 Auslöser



REQ.FA.DoFwDownload.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Durch das SMGW, sobald der Download Startzeitpunktes des Firmware-Update-Profiles erreicht wurde (siehe ▸FA.UpdateFwUpdateConfig und ▸Firmware-Update-Profil).

▸ [BSI.18002.0]

3.20.4.3 Anforderungen

- Das SMGW **SOLL** den Datei-Download über das Kommunikationsszenario ▸WKS.DOWNLOAD durchführen. [REQ.FA.DoFwDownload.20].
- Sofern gemäß ▸ICS.FA.DoFwDownload.10 kein Datei-Download über ▸WKS.DOWNLOAD implementiert ist **MUSS** das SMGW den Datei-Download über das Kommunikationsszenario ▸WKS.ADMIN-SERVICE durchführen (Siehe ▸ICS.FA.DoFwDownload.20). [REQ.FA.DoFwDownload.30]
- Das SMGW **MUSS** bei Abbruch des Downloads die Verbindung gemäß zugeordnetem WAN-Kommunikationsprofil erneut aufbauen und den Datei-Download fortsetzen. ▸ [BSI.18002.1] [REQ.FA.DoFwDownload.40] Ein Abbruch kann durch Timeout der Datenübertragung, durch einseitige Beendigung der TLS-Verbindung oder durch Fehler des Dateiservers stattfinden.
- (▸ICS.FA.DoFwDownload.30) Das SMGW **SOLL** die erfolgreich heruntergeladene Datei bis zur erfolgreichen Installation, auch über einen Neustart hinweg, persistieren. [REQ.FA.DoFwDownload.70]
- Sofern die Geräte-ID im Datenfeld ▸deviceId das SMGW identifiziert, **MUSS** das SMGW nach erfolgreichem Download und nach Erreichen des Installationszeitpunktes ▸timeOfActivation die Installation/Aktivierung (siehe ▸FA.DoFwActivation) starten. [REQ.FA.DoFwDownload.50]
- (▸ICS.FAKAT.ValProcBilling.20) Sofern die Geräte-ID im Datenfeld ▸deviceId eine Messeinrichtung identifiziert, **MUSS**+ das SMGW nach erfolgreichem Download und nach Erreichen des Installationszeitpunktes ▸timeOfActivation die Übertragung in die Messeinrichtung starten (siehe ▸FA.ExportFileToMtr). ▸ [BSI.18011.0] ▸ [BSI.18011.1] [REQ.FA.DoFwDownload.60]

ICS



ICS.FA.DoFwDownload.10

Der GWH **MUSS** im ICS erklären, ob das SMGW den Datei-Download über ▸WKS.DOWNLOAD (ohne CMS-Inhaltsdatenverschlüsselung) unterstützt.



ICS.FA.DoFwDownload.20

Der GWH **MUSS** im ICS erklären, ob das SMGW den Datei-Download über ▸WKS.ADMIN-SERVICE (mit CMS-Inhaltsdatenverschlüsselung) unterstützt.



ICS.FA.DoFwDownload.30

Der GWH **MUSS** im ICS erklären, ob das SMGW die heruntergeladene Datei (Firmware) über einen Neustart des SMGW hinweg persistiert.

3.20.4.4 Implementierungshinweise

Wird der Download unterbrochen, sollten die bereits übertragenen Teile der Firmware-Datei nicht gelöscht werden, so dass bei einem Fortsetzen des Downloads bereits übertragene Daten nicht erneut übertragen werden.

Bei Verwendung von WKS.DOWNLOAD ist die Datei ergänzend zur TLS-Sicherung im WAN mit einem Signatur-Verfahren gemäß [TR-03109-3] vom Hersteller signiert (Siehe ▸ICS.FA.DoFwDownload.10).

3.20.5 FA.DoFwActivation

3.20.5.1 Beschreibung

Aktiviert eine vollständig heruntergeladene Firmware-Datei, so dass sie künftig in der zu aktualisierenden Komponente genutzt wird. Das zugrundeliegende Firmware-Update-Profil legt dabei das Ziel zur Aktivierung der Firmware-Datei fest. Dieses Ziel kann das SMGW selbst oder eine verbundene Messeinrichtung sein.

Ist das Ziel das SMGW, erfolgt vor Aktivierung eine Prüfung der Integrität und Authentizität der Firmware-Datei. Firmware-Dateien für andere Ziele werden durch das SMGW nicht auf Integrität oder Authentizität überprüft. Das SMGW stellt in diesem Fall lediglich die Integrität und Authentizität auf dem Übertragungsweg sicher.

Während der Firmware-Aktivierung können Dienste und Funktionen der zu aktualisierenden Komponente nicht verfügbar sein.

Nach erfolgreicher Aktivierung der Firmware wird das Firmware-Update-Profil vom SMGW gelöscht.

Sofern sich die Aktivierung auf das SMGW bezieht, kann der FA einen Neustart des SMGW auslösen, sofern dies bei der jeweiligen Implementierung notwendig ist.

Für die Dauer der Aktivierung wird eine Obergrenze gesetzt, die so gewählt wurde, dass höchstens ein viertelstündlich registrierter Messwert fehlt und eine Planbarkeit für die kommunikative Wiedererreichbarkeit der GWA-Systeme gegeben ist.

3.20.5.2 Auslöser



REQ.FA.DoFwActivation.5

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Durch das SMGW, sobald der Installations-Startzeitpunkt eines Firmware-Update-Profiles der ▸deviceId des SMGW entspricht, nach erfolgreichem Download erreicht wurde (siehe ▸FA.UpdateFwUpdateConfig und ▸Abschnitt 3.22.18).

▸ [BSI.18008.0]

3.20.5.3 Anforderungen

- Sofern das SMGW Ziel der Aktivierung ist, **MUSS** das SMGW eine Aktivierung ablehnen, wenn die Integrität der Firmware oder die Authentizität der Firmware nicht validiert werden kann. ▸ [BSI.18008.1] [REQ.FA.DoFwActivation.10]
- Sofern das SMGW Ziel der Aktivierung ist, **MUSS** das SMGW eine Aktivierung der Firmware ablehnen, die nicht kompatibel mit der Gerätetyp-Hardware oder der installierten Firmware-Umgebung ist. ▸ [BSI.18008.2] [REQ.FA.DoFwActivation.20]
- Sofern der Installations-Startzeitpunkt vor dem Ende des erfolgreichen Downloads liegt, **MUSS** das SMGW die Installation bis zum erfolgreichen Download verzögern. [REQ.FA.DoFwActivation.25]
- Das SMGW **MUSS** die Installation der Firmware durchführen. ▸ [BSI.18009.0] ▸ [BSI.18009.1] ▸ [BSI.18019.0] ▸ [BSI.18019.1] [REQ.FA.DoFwActivation.60]
- Sofern das SMGW Ziel der Aktivierung ist, **SOLL** das SMGW spätestens 14 Minuten nach Auslösen der Aktivierung Zählerstände registrieren können. (▸ICS.FA.DoFwActivation.10) [REQ.FA.DoFwActivation.40]
- Sofern das SMGW Ziel der Aktivierung ist, **SOLL** das SMGW spätestens 14 Minuten nach Auslösen der Aktivierung eine Kommunikationsverbindung zum GWA (via ▸WKS.WAKEUP, ▸WKS.MANAGEMENT oder ▸WKS.ADMIN-SERVICE) aufbauen können. (▸ICS.FA.DoFwActivation.10) [REQ.FA.DoFwActivation.50]

ICS



ICS.FA.DoFwActivation.10

Der GWH **MUSS** im ICS beschreiben, ob die Firmware-Aktivierung im SMGW länger als 14 Minuten dauern kann.



ICS.FA.DoFwActivation.20

Der GWH **MUSS** im ICS in Minuten angeben (aufgerundet), wie lang die Aktivierung einer Firmware im SMGW nach erfolgreichem Download dauern kann.

3.20.5.4 Implementierungshinweise

Aus Gründen der herstellerübergreifenden Interoperabilität kann die Firmwaresignatur mit CMS-SignedData gemäß [DS] Kapitel "CMS - Cryptographic Message Syntax" mit einem Signaturverfahren gemäß [TR-03109-3] verwendet werden.

3.20.6 FA.UpdateFwUpdateConfig

3.20.6.1 Beschreibung

Das SMGW erhält im Aufrufparameter ▸Abschnitt 3.22.18 die Konfigurationsdaten, um beispielsweise zeitgesteuert automatisch eine Datei vom Fileserver zu laden und im SMGW zu installieren oder an eine Messeinrichtung zu übertragen.

Der Aufruf ist nur möglich, wenn nicht bereits ein Update für das im FwUpdateProfil identifizierte Gerät gestartet wurde.

3.20.6.2 Auslöser



REQ.FA.UpdateFwUpdateConfig.5

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.20.6.3 Anforderungen

- Das SMGW **MUSS** den Import des Firmware-Update-Profiles ablehnen, wenn das Datenfeld ▸deviceId nicht der SMGW-ID entspricht und das SMGW das Senden von Dateien an Messeinrichtungen gemäß ▸ICS.FAKAT.MtrServices.10 nicht unterstützt. ▸ [BSI.18001.1] [REQ.FA.UpdateFwUpdateConfig.40]
- Das SMGW **MUSS** den Import ablehnen, wenn das Datenfeld ▸deviceId nicht der SMGW-ID oder einer ▸meterId einer über LKS1 kommunikativ angebundenen Messeinrichtung entspricht. ▸ [BSI.18001.1] [REQ.FA.UpdateFwUpdateConfig.30]
- Das SMGW **MUSS** den Download zum konfigurierten Zeitpunkt beginnen. ▸ [BSI.18001.0] [REQ.FA.UpdateFwUpdateConfig.20]

3.20.7 FA.ReadFwUpdateConfig

3.20.7.1 Beschreibung

Exportiert das konfigurierte und über den Aufrufparameter identifizierte Firmware-Update-Profile an den Aufrufer.

3.20.7.2 Auslöser



REQ.FA.ReadFwUpdateConfig.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.20.7.3 Anforderungen

Das SMGW **MUSS** das konfigurierte Firmware-Update-Profile gemäß ▸Abschnitt 3.22.18 an den Aufrufer exportieren. [REQ.FA.ReadFwUpdateConfig.20]

3.20.8 FA.DeleteFwUpdateConfig

3.20.8.1 Beschreibung

Ein Download, der dem über das im Aufruf identifizierte Firmware-Update-Profil zugeordnet ist, wird beendet und das Firmware-Update-Profil sowie alle zugehörigen, bereits geladenen Datei-Artefakte werden gelöscht.

3.20.8.2 Auslöser



REQ.FA.DeleteFwUpdateConfig.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- (▸deviceId einer Messeinrichtung) Löschen eines LMN-Kommunikationsprofils, dessen Geräte-ID mit einem Firmware-Update-Profil verknüpft ist.
- (▸deviceId einer Messeinrichtung) Nach erfolgreicher Installation der Firmware in der Messeinrichtung (▸FA.ExportFileToMtr).
- (▸deviceId des SMGW) Nach erfolgreicher Installation der Firmware im SMGW (▸FA.DoFwActivation)

3.20.8.3 Anforderungen

Das SMGW **MUSS** einen laufenden Datei-Download beenden, keine Installation einer heruntergeladenen Datei durchführen und das konfigurierte Firmware-Update-Profil löschen. ▸ [BSI.18002.1] [REQ.FA.DeleteFwUpdateConfig.20]

3.20.8.4 Implementierungshinweise

Eventuell vorhandene bereits heruntergeladene Dateien zu diesem Firmware-Update-Profil werden gelöscht. Eine möglicher, nachfolgender Download der Datei lädt somit alle Daten erneut vom Dateiserver.

3.21 Netzwerkdiagnose (FAKAT.NetworkDiagnosis)

3.21.1 Übersicht

Diese Anwendungsfälle dienen dem Betreiber des SMGW und der damit verbundenen Kommunikationsnetze zur Unterstützung der Diagnose und Behebung von Kommunikationsproblemen.

Der Einsatz eines SMGW erfordert eine zuverlässige Anbindung an ein Weitverkehrsnetz an der WAN-Schnittstelle. Mit der steigenden Verbreitung von SMGW wächst auch der Wunsch der Messstellenbetreiber nach einer Möglichkeit, die Qualität der WAN-Anbindung aller ausgerollten SMGW über die Nutzungsdauer überwachen zu können und bei Unregelmäßigkeiten informiert zu werden. Der WAN-Kommunikationsadapter[18] verfügt in der Regel über Status- oder Diagnoseinformationen zur Netzwerkverbindung (z.B. den Signalrauschabstand, die verwendete Mobilfunktechnologie oder die IP-Adresse). Diese Daten werden im Folgenden als "Netzwerkdiagnosedaten" bezeichnet.

Der Begriff "Netzwerkdiagnoseservice" (NDS) beschreibt hingegen die benötigten Funktionen im SMGW, um Netzwerkdiagnosedaten periodisch oder aufgrund bestimmter Ereignisse aus dem WAN-Kommunikationsadapter auszulesen und an einen autorisierten EMT oder den GWA als Empfänger zu versenden.

Der Netzwerkdiagnoseservice des SMGW wird durch den GWA eingerichtet. Hierfür spielt der GWA ein spezielles Netzwerkdiagnoseprofil ins SMGW ein, welches Informationen darüber beinhaltet, welche Daten an welchen berechtigten Empfänger übertragen werden und wie die Übertragung ausgelöst wird. Neben einer periodischen Übertragung von Netzwerkdiagnosedaten durch das SMGW (Push) ist auch eine Übertragung nach der Verletzung definierter Schwellwertkriterien oder auf Veranlassung des GWA (Pull) möglich.

[18] Im Rahmen der Beschreibung des Netzwerkdiagnoseservice bezieht sich der Begriff "WAN-Kommunikationsadapter" auf die technische Komponente des SMGW, die dem Netzwerkzugang dient. Dies kann beispielsweise ein Mobilfunkmodem oder eine physische Ethernet Schnittstelle sein.

Die Konfiguration des Netzwerkdiagnoseservices erfolgt über das Kommunikationsszenario MANAGEMENT, der Versand an einen EMT über das Kommunikationsszenario INFO-REPORT und der Versand an den GWA über das Kommunikationsszenario ADMIN-SERVICE.

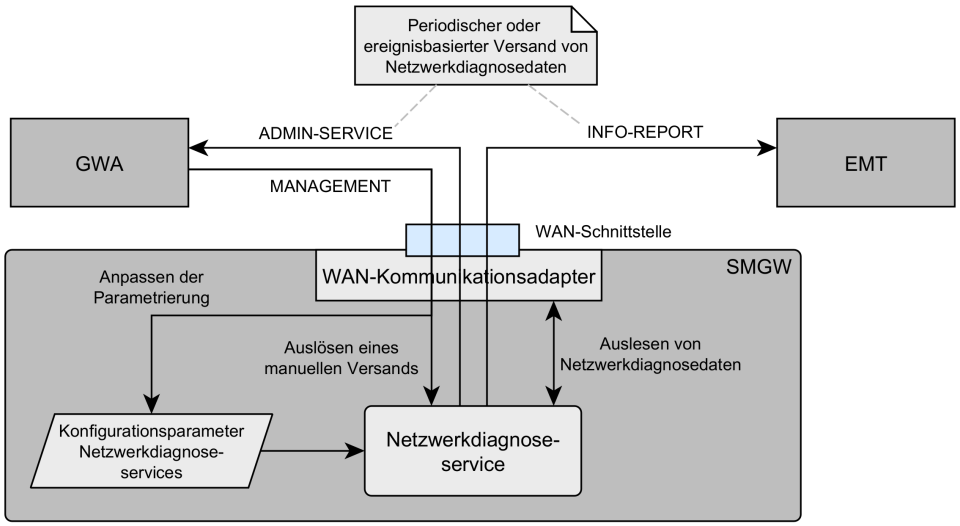


Abbildung 3.21. Übersicht der verwendeten Kommunikationsszenarien

▸Tabelle 3.61 enthält eine Übersicht der FA zur Netzwerkdiagnose.

3.21.2 Übersicht der FA

Aufgabe	Umsetzung
Versand von Diagnosedaten der Netzwerkschnittstelle ausgelöst durch den GWA	Das SMGW **KANN** ▸FA.DoNdsNotification für den GWA umsetzen (▸ICS.NDS.Umsetzung.10). [REQ.FAKAT.SmgwOperation.110]
Konfiguration zur Netzwerkdiagnose importieren	Das SMGW **KANN** ▸FA.CreateNdsConfig für den GWA umsetzen (▸ICS.NDS.Umsetzung.10). [REQ.WAN.Management.300]
Konfiguration zur Netzwerkdiagnose aktualisieren	Das SMGW **KANN** ▸FA.UpdateNdsConfig für den GWA umsetzen (Bedingung: ▸ICS.NDS.Umsetzung.10). [REQ.WAN.Management.301]
Konfiguration zur Netzwerkdiagnose löschen	Das SMGW **KANN** ▸FA.DeleteNdsConfig für den GWA umsetzen (▸ICS.NDS.Umsetzung.10). [REQ.WAN.Management.302]
Konfiguration zur Netzwerkdiagnose auslesen	Das SMGW **KANN** ▸FA.ReadNdsConfig für den GWA umsetzen (▸ICS.NDS.Umsetzung.10). [REQ.WAN.Management.303]

Tabelle 3.61 Übersicht der FA der Kategorie FAKAT.NetworkDiagnosis

ICS

ICS.NDS.Umsetzung.10

Der GWH **MUSS** im ICS angeben, ob das SMGW einen Netzwerkdiagnoseservice gemäß ▸FAKAT.NetworkDiagnosis implementiert.

ICS.NDS.Lebenszyklus.10

Der GWH **MUSS** im ICS angeben, ob das SMGW den Netzwerkdiagnoseservice in der Phase "Personalisierung" bereitstellen kann.

3.21.3 Datenstrukturen

Das NDS-Konfigurationsprofil ist in ▸Abschnitt 3.22.30 beschrieben.

Die Datenstruktur mit den NDS-Statusinformationen ist in ▸Abschnitt 3.22.32 beschrieben.

Die zulässigen konfigurierbaren und exportierbaren NDS-Statusinformationen sind in ▸Abschnitt 3.22.31 beschrieben.

3.21.4 FA.DoNdsNotification

3.21.4.1 Beschreibung

Der Netzwerkdiagnoseservice erlaubt die Bereitstellung von Status- und Diagnoseinformationen über die WAN-Verbindung des SMGW für den GWA oder einen EMT. Grundsätzlich sind auf Basis der durch den GWH gewählten Sicherheitsarchitektur auch andere Umsetzungen zur Bereitstellung von Netzwerkdiagnosedaten (bspw. PP-konform als Dienst des im Gehäuse des SMGW befindlichen separierten WAN-Kommunikationsadapters) möglich.

3.21.4.2 Auslöser

REQ.FA.DoNdsNotification.10

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.
- Einmalig bei Überschreiten/Unterschreiten eines mit dem Netzwerkdiagnose-Konfigurationsprofil parametrierten Schwellwertes.
- Start des SMGW gemäß Netzwerkdiagnose-Konfigurationsprofil.
- Einspielen eines Netzwerkdiagnose-Konfigurationsprofils mit ▸FA.CreateNdsConfig.
- Periodisch gemäß Netzwerkdiagnose-Konfigurationsprofil.

3.21.4.3 Anforderungen

- Falls das SMGW einen Netzwerkdiagnoseservice gemäß ▸ICS.NDS.Umsetzung.10 umsetzt, **MUSS** das SMGW gemäß eines Konfigurationsprofiles ereignisgesteuert Informationen zur Diagnose der Qualität der kommunikativen Netzwerkanbindung ausliefern können. [REQ.WAN.EmtBenachrichtigung.40]
- Falls das SMGW einen Netzwerkdiagnoseservice gemäß ▸ICS.NDS.Umsetzung.10 umsetzt, **MUSS** das SMGW einen Dienst beim GWA nutzen können, um Netzwerkdiagnosedaten an den GWA zu übertragen. [REQ.WAN.ZugriffAufGwaDienste.50]
- Das SMGW **MUSS** zum Versandzeitpunkt aktuelle Werte für die parametrierte Teilmenge der Netzwerkdiagnosedaten aus dem WAN-Kommunikationsadapter auslesen und unter Verwendung der Datenstruktur aus ▸Abschnitt 3.22.32 an den parametrierten berechtigten Empfänger versenden. [REQ.FA.DoNdsNotification.20]
- Das SMGW **MUSS** für den Versand an den GWA das Kommunikationsszenario ADMIN-SERVICE und für den Versand an einen EMT das Kommunikationsszenario INFO-REPORT verwenden. [REQ.FA.DoNdsNotification.30]
- Das SMGW **MUSS** in der Phase "Normalbetrieb" die Wirkzertifikate des SMGW beim Aufbau von Kommunikationskanälen zum Zweck des Versands von Netzwerkdiagnosedaten verwenden. [REQ.FA.DoNdsNotification.70]
- Das SMGW **MUSS** Schwellwertverletzungen auf Basis des Konfigurationsparameters "Schwellwerte" spätestens zu jedem Versandzeitpunkt erkennen. [REQ.FA.DoNdsNotification.130]
- Wenn mehrere Versandauslöser gleichzeitig auftreten, **MUSS** das SMGW sicherstellen, dass nur ein Datenversand stattfindet. [REQ.FA.DoNdsNotification.140]
- Das SMGW **MUSS** sicherstellen, dass die Datenstruktur beim Versand den Versandauslöser mit der höchsten Priorität enthält, wenn mehrere Versandauslöser gleichzeitig auftreten. Die Reihenfolge der Auflistung der möglichen Versandauslöser in ▸Abschnitt 3.22.32 entspricht einer absteigenden Priorität. [REQ.FA.DoNdsNotification.150]

Periodischer Versand

Der periodische Versand von Netzwerkdiagnosedaten verwendet, abhängig von den gesetzten Konfigurationsparametern und den derzeit vorliegenden Bedingungen, unterschiedliche Intervalle zur Bestimmung von Versandzeitpunkten.

Ein Versandzeitpunkt gilt auch dann als solcher, wenn der Versand zu diesem Zeitpunkt nicht oder nicht erfolgreich durchgeführt werden konnte.

Das SMGW **MUSS** das zu verwendende Intervall für den periodischen Versand nach folgendem Ablauf bestimmen: [REQ.FA.DoNdsNotification.160]

- Wenn Schwellwerte für Netzwerkdiagnosedaten vom SMGW implementiert werden und das Intervall nach dem Konfigurationsparameter "Intervall Schwellwert" verwendet werden soll (s. ▸REQ.FA.DoNdsNotification.120 in ▸Abschnitt 3.21.4.3), dann **MUSS** das SMGW genau dieses Intervall verwenden. [REQ.FA.DoNdsNotification.170]
- Wenn der Konfigurationsparameter "Gültigkeit Intervall nach Start" angegeben ist und die Dauer seit dem letzten Start des SMGW geringer ist als im Konfigurationsparameter "Gültigkeit Intervall nach Start" angegeben, **MUSS** das SMGW das Intervall nach dem Konfigurationsparameter "Intervall nach Start" verwenden. [REQ.FA.DoNdsNotification.180]
- Wenn der Konfigurationsparameter "Intervall periodisch" angegeben ist, **MUSS** das SMGW genau dieses Intervall verwenden. [REQ.FA.DoNdsNotification.190]
- Wenn keine der vorherigen Bedingungen zutrifft, **MUSS** das SMGW den periodischen Versand deaktivieren. [REQ.FA.DoNdsNotification.200]
- Das SMGW **KANN** einem berechtigten Empfänger im Rahmen des Versands die Netzwerkdiagnosedaten aus ▸Abschnitt 3.22.31 oder eine Teilmenge davon bereitstellen. [REQ.FAKAT.NetworkDiagnosis.50]
- Bei Erzeugung einer Datenstruktur für den Versand (s. ▸Tabelle 3.95) **MUSS** das SMGW den in der Spalte "Attributname" aus ▸Abschnitt 3.22.31 angegebenen Wert für die Identifikation der Daten im Parameter "Werte der Netzwerkdiagnosedaten" verwenden. [REQ.FAKAT.NetworkDiagnosis.60]

▸Abbildung 3.22 zeigt die Versandzeitpunkte in einem beispielhaften, zeitlichen Verlauf auf Basis der obigen Beschreibung. Voraussetzung ist, dass zuvor ein gültiges Netzwerkdiagnoseprofil eingespielt wurde. Im Beispiel wird davon ausgegangen, dass die optionalen Konfigurationsparameter "Intervall Start", "Intervall periodisch", "Intervall Schwellwert", "Gültigkeit Intervall Start", "Gültigkeit Intervall Schwellwert" und "Schwellwerte" angegeben sind. Weiterhin tritt im Beispiel die Schwellwertverletzung für einen Zeitraum auf, der kürzer ist als der Wert von "Gültigkeit Intervall Schwellwert".

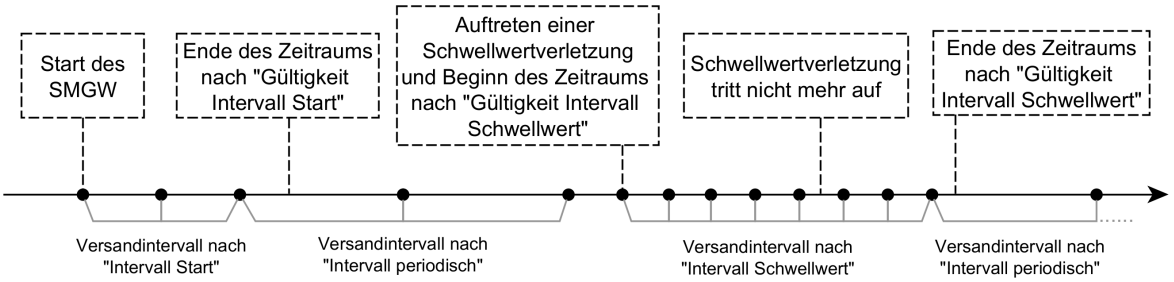


Abbildung 3.22. Beispiel verschiedener Versandzeitpunkte im zeitlichen Verlauf

Versand auf Basis von Schwellwerten

Optional können Schwellwerte für numerische Netzwerkdiagnosedaten implementiert werden, die einen Versand auslösen, wenn eine Schwellwertverletzung (Über- oder Unterschreitung) auftritt. Sofern das SMGW Schwellwerte für Netzwerkdiagnosedaten implementiert, sind die Anforderungen dieses Kapitels normativ und vom SMGW zu erfüllen.

Sobald das SMGW mindestens eine Schwellwertverletzung auf Basis des Konfigurationsparameters "Schwellwerte" erkennt, **MUSS** das SMGW die Netzwerkdiagnosedaten einmalig versenden. [REQ.FA.DoNdsNotification.90] Wenn der Konfigurationsparameter "Intervall Schwellwert" angegeben ist, **MUSS** das SMGW eben dieses Intervall für den periodischen Versand verwenden. [REQ.FA.DoNdsNotification.100]

Treten weitere Schwellwertverletzungen auf, während das Intervall nach Konfigurationsparameter "Intervall Schwellwert" verwendet wird, **DARF** das SMGW **KEINEN** zusätzlichen Versand auslösen. Dies gilt sowohl für eine erneute Schwellwertverletzung desselben Netzwerkdiagnosedatums als auch eines anderen Netzwerkdiagnosedatums. [REQ.FA.DoNdsNotification.110]

Das SMGW **MUSS** das Intervall nach Konfigurationsparameter "Intervall Schwellwert" solange verwenden, bis mindestens eine der folgenden Bedingungen erfüllt ist: [REQ.FA.DoNdsNotification.120]

- Das SMGW wird neugestartet.
- Der Konfigurationsparameter "Gültigkeit Intervall Schwellwert" ist nicht angegeben und es tritt keine Schwellwertverletzung mehr auf.
- Der Konfigurationsparameter "Gültigkeit Intervall Schwellwert" ist angegeben und das Intervall nach Konfigurationsparameter "Intervall Schwellwert" wurde mindestens für eine Dauer verwendet, die dem Konfigurationsparameter "Gültigkeit Intervall Schwellwert" entspricht, und es tritt keine Schwellwertverletzung mehr auf.

Das SMGW **SOLL** für die Auslieferung bei Verwendung des WKS ADMIN-SERVICE Kommunikationsszenarios den Point of Contact gemäß WAN-Kommunikationsprofil verwenden. [REQ.FA.DoNdsNotification.220]

Das SMGW **SOLL** für die Auslieferung bei Verwendung des WKS INFO-REPORT Kommunikationsszenarios den Point of Contact gemäß WAN-Kommunikationsprofil verwenden. [REQ.FA.DoNdsNotification.230]

NDS in der Phase Personalisierung

- Das SMGW **DARF** dem GWA in der Phase "Personalisierung" **NICHT** die Möglichkeit bieten, einen "vom GWA verursachten Versand" auszulösen. [REQ.FA.DoNdsNotification.40]
- Wenn sich das SMGW in der Phase "Personalisierung" befindet und mindestens ein Empfänger für Netzwerkdiagnosedaten parametriert ist, **MUSS** das SMGW den GWA nach jedem Neustart durch einen Eintrag im System-Log über alle konfigurierten Empfänger (Common Name des TLS-Zertifikats) informieren. [REQ.FA.DoNdsNotification.50]
-
- Das SMGW **MUSS** in der Phase "Personalisierung" die Gütesiegelzertifikate des SMGW beim Aufbau von Kommunikationskanälen zum Zweck des Versands von Netzwerkdiagnosedaten verwenden. [REQ.FA.DoNdsNotification.60]

ICS

Ein Versand von Netzwerkdiagnosedaten fällt nicht unter den zu protokollierenden Datenverkehr, da die enthaltenen Daten den Anschlussnutzer nicht betreffen. Das SMGW kann den Datenverkehr im Zusammenhang mit dem Netzwerkdiagnoseservice dennoch im Anschlussnutzer-Log und System-Log protokollieren.



ICS.NDS.Schwellwerte.10

Der GWH **MUSS** im ICS angeben, ob er die Übermittlung von Netzwerkdiagnosedaten auf Basis von Schwellwerten unterstützt.



ICS.NDS.Versand.10

Der GWH **MUSS** im ICS angeben, welche Versandauslöser vom SMGW zusätzlich implementiert werden.



ICS.NDS.Uri.20

Der GWH **MUSS** im ICS angeben, ob das SMGW den Point of Contact aus dem WAN-Kommunikationsprofil gemäß ▸REQ.FA.DoNdsNotification.220 verwendet.



ICS.NDS.Uri.21

Sofern das SMGW gemäß ▸ICS.NDS.Uri.20 nicht den Point of Contact aus dem WAN-Kommunikationsprofil verwendet, **MUSS** der GWH vorhandene Abweichungen im ICS beschreiben.



ICS.NDS.Uri.30

Der GWH **MUSS** im ICS angeben, ob das SMGW den Point of Contact aus dem WAN-Kommunikationsprofil gemäß ▸REQ.FA.DoNdsNotification.230 verwendet.



ICS.NDS.Uri.31

Sofern das SMGW gemäß ▸ICS.NDS.Uri.30 nicht den Point of Contact aus dem WAN-Kommunikationsprofil verwendet, **MUSS** der GWH vorhandene Abweichungen im ICS beschreiben.

3.21.4.4 Implementierungshinweise

Der Versand auf Veranlassung durch den GWA erfolgt zusätzlich zum periodischen Versand, weshalb der zugehörige Zeitpunkt des Versands nicht als "letzter Versandzeitpunkt" für die Bestimmung der periodischen Versandzeitpunkte berücksichtigt wird. Dies gilt unabhängig vom derzeit verwendeten Intervall für den periodischen Versand (normal, nach Start, bei Schwellwertverletzung).

3.21.5 FA.CreateNdsConfig

3.21.5.1 Beschreibung

Das SMGW prüft, persistiert und aktiviert die Konfigurationsdaten gemäß ▸Netzwerkdiagnose-Konfigurationsprofil, die die Übermittlung von Netzwerkdiagnosedaten an GWA oder EMT festlegen.

3.21.5.2 Auslöser



REQ.FA.CreateNdsConfig.40

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.21.5.3 Anforderungen

- Das SMGW **MUSS** das Anlegen ablehnen, sofern bereits ein Netzwerkdiagnose-Kommunikationsprofil mit gleicher Profil-Id im SMGW existiert. [REQ.FA.CreateNdsConfig.10]
- Das SMGW **MUSS** das Anlegen ablehnen, sofern mindestens ein Attributname angegeben ist, das nicht in ▸Abschnitt 3.22.31 und nicht im ▸ICS.FAKAT.NetworkDiagnosis.20 beschrieben ist. [REQ.FA.CreateNdsConfig.11]
- Das SMGW **MUSS** mindestens die Parametrierung eines Netzwerkdiagnoseprofils für einen (1) Empfänger unterstützen. [REQ.FA.CreateNdsConfig.30] [19]

3.21.5.4 Implementierungshinweise

Sofern WAN-Kommunikationsprofile für den Netzwerkdiagnoseservice als Teil der initialen Konfiguration eingespielt wurden und die Konfiguration der SMGW-Zertifikate innerhalb des WAN-Kommunikationsprofils erfolgt, muss das SMGW diese WAN-Kommunikationsprofile beim Wechsel in die Phase "Normalbetrieb" aktualisieren, sodass dort die Gütesiegelzertifikate des SMGW durch die Wirkzertifikate des SMGW ersetzt oder gelöscht werden.

3.21.6 FA.UpdateNdsConfig

3.21.6.1 Beschreibung

Das SMGW speichert die aktualisierten Konfigurationsdaten gemäß ▸Abschnitt 3.22.30 , die die Übermittlung von Netzwerkdiagnosedaten an GWA oder EMT festlegen.

[19] Die nachfolgende Beschreibung geht von genau einem Empfänger aus. Können Netzwerkdiagnoseprofile für mehrere Empfänger eingebracht werden, gelten die beschriebenen Anforderungen jeweils pro Empfänger.

3.21.6.2 Auslöser



REQ.FA.UpdateNdsConfig.30

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.21.6.3 Anforderungen

- Das SMGW **MUSS** die Aktualisierung ablehnen, wenn das referenzierte WAN-Kommunikationsprofil oder die Profil-Id geändert würde. [REQ.FA.UpdateNdsConfig.10]
- Das SMGW **MUSS** die Aktualisierung ablehnen, wenn zwar "durationThreshold", aber nicht "intervalThreshold" angegeben ist. [REQ.FA.UpdateNdsConfig.11]
- Das SMGW **MUSS** das im Aufrufparameter identifizierte Netzwerkdiagnose-Konfigurationsprofil aktualisieren und persistieren. [REQ.FA.UpdateNdsConfig.20]

3.21.7 FA.DeleteNdsConfig

3.21.7.1 Beschreibung

Das SMGW löscht die Konfigurationsdaten, die die Übermittlung von Netzwerkdiagnosedaten an GWA oder EMT festlegen. Die Übermittlung von Netzwerkdiagnosedaten an GWA oder EMT wird beendet.

3.21.7.2 Auslöser



REQ.FA.DeleteNdsConfig.30

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.21.7.3 Anforderungen

- Das SMGW **MUSS** das im Aufrufparameter identifizierte Netzwerkdiagnose-Konfigurationsprofil im SMGW löschen. [REQ.FA.DeleteNdsConfig.10]
- Das SMGW **DARF** den Versand von Netzwerkdiagnosedaten **NICHT** weiter durchführen, wenn das Netzwerkdiagnoseprofil entfernt wurde. [REQ.FA.DeleteNdsConfig.20]

3.21.8 FA.ReadNdsConfig

3.21.8.1 Beschreibung

Der GWA exportiert das im Aufrufparameter referenzierte Netzwerkdiagnose- Konfigurationsprofil.

3.21.8.2 Auslöser



REQ.FA.ReadNdsConfig.20

Das SMGW **MUSS** diesen FA bei folgenden Ereignissen auslösen:

- Empfang einer Anfrage über ▸WKS.MANAGEMENT.

3.21.8.3 Anforderungen

Das SMGW **MUSS** das im Aufrufparameter identifizierte Netzwerkdiagnose-Konfigurationsprofil gemäß ▸Abschnitt 3.22.30 an den Aufrufer übermitteln. [REQ.FA.ReadNdsConfig.10]

3.22 Datenstrukturen und Profile

3.22.1 Datenfelder in Profilen

Namen von Datenfeldern sind in einer deutschen Schreibweise angegeben. Für technische Zwecke und zur einfacheren Referenzierbarkeit in dieser Technischen Richtlinie folgt dem Namen in Klammern eine kürzere englische Form.

Die Reihenfolge von Datenfeldern in Datenstrukturen oder Parametern in Profilen ist für die Umsetzung an den Schnittstellen nicht bindend.

Der Datentyp wird nur für Informationen (Profile und Datenstrukturen), die an den Schnittstellen des SMGW interoperabel ausgetauscht werden, angegeben (Siehe ▸Abschnitt 3.22.2).

Sollte ein Datenfeld oder Parameter optional sein, wird an seinen Namen das Suffix (optional) angehängt. Die Beschreibung enthält dann bei Konfigurationsprofilen eine Aussage, welcher Default-Wert vom SMGW verwendet werden soll. Optionalität bezieht sich auf das Vorhandensein eines Datenfeldes oder Parameters in der Datenstruktur, nicht auf die Implementierung der zugeordneten Funktionalität.

Ist ein Datenfeld oder Parameter optional und kann dieses Datenfeld nicht auf ein Datenfeld der API (siehe [TR-03109-1-II]) abgebildet werden, dann gilt der für das Datenfeld beschriebene Standardwert.

Das SMGW **MUSS** beim Import von Konfigurationsprofilen jeweils den Standardwert bei fehlenden optionalen Parametern annehmen. [REQ.Profile.10]

3.22.2 Datentypen

Datentyp Name	Bedeutung	Wertebereich
Number	Eine Gleitkommazahl	binary64 nach [IEEE 754][20]
Integer (m..n)	Eine Ganzzahl zwischen m und n	$-(2^{31}) <= m <= n <= 2^{31}-1$
String	Eine Zeichenkette	Gemäß Format (siehe unten)
Boolean	Ein Wahrheitswert	-
Enumeration	Eine Aufzählung von möglichen Werten	-
Array [x..y] von ...	Eine Reihung von Elementen eines bestimmten Datentyps mit mindestens x und maximal y Elementen	0 <= x <= y <= 2.000.000
Tupel	Ein Element, das aus mehreren weiteren Elementen potenziell unterschiedlicher Datentypen besteht	-
Any	Beliebiger Datentyp, um die Erweiterbarkeit der Datenstruktur zur ermöglichen	-

Tabelle 3.62 Übersicht über die in Profilen verwendeten Datentypen

Sofern Wertebereiche oder Formate eingeschränkt werden, wird dies in Klammern nach dem Datentyp angegeben.

Format-spezifische Einschränkungen für String:

- (dateTime): Datum und Zeit im "date-time"-Format gemäß [RFC3339] (Trenner "T") (UTC)
- (date): Datum im "full-date"-Format gemäß [RFC3339]
- (time): Tageszeit im "partial-time"-Format (UTC) gemäß [RFC3339]
- (hexString): (Binäre) Daten in Base16-Codierung (Siehe [RFC4648]) bei einer maximalen Länge von 10000 Zeichen

[20] Dies betrifft ausschließlich den verwendeten Wertebereich (häufig auch als "double" bezeichnet). Die verwendete Darstellung und Kanonisierung im Rahmen der API wird in der Detailspezifikation festlegt.

- (obis): OBIS-IDs werden im Format A-B:C.D.E[*F] notiert. Die Wertegruppen A-F werden als dezimale Ganzzahlen (0-255) ohne führende "0" notiert (Siehe ▸Abschnitt 2.5.2). Die Wertegruppe F kann entfallen, wenn sie den Wert 255 hat.
- (huid): 14-stellige Geräteidentifikation gemäß [DIN43849] (ohne Leerzeichen)
- (name): Max. 63-stellige Identifikation mit den Zeichen "A" bis "Z", "-", ".", "0" bis "9"
- (1..n): Einschränkung der Stringlänge ohne definiertes Format mit n <= 500
- (m..n) für Integer: Die Unter- und Obergrenze des Wertebereiches (inklusive des Grenzwertes). Fehlt die Obergrenze ("n"), wird 2^{31}-1 verwendet.
- (ipv4): IPv4 Adresse in Network Byte Order ohne führende Nullen: "0".."255" "." "0".."255" "." "0".."255" "." "0".."255"
- (absolute-uri): Eine absolute URI gemäß [RFC3986]. Parameterabhängig kann das Format weiter eingeschränkt werden.
- (event): Ereigniscode gemäß <vendor "AAA".."ZZZ">.<eventid "0"..2^{32}-1>.<eventsubid "0"..2^{8}-1>>

Number und Integer können durch (x..y) im Wertebereich auf Werte zwischen x und y (inklusive) eingeschränkt sein.

3.22.3 Datenstrukturen mit Spaltenüberschriften

Einige der Datenstrukturen dieser TR verwenden zur Optimierung des Datenvolumens ein Datenfeld "Spalten" (columns). Dies gilt beispielsweise für die in der Messwertverarbeitung und dem Messwertversand verwendeten Listen (RWL, AWL, NWL, TWL). Ziel des Datenfelds ist die Redundanz der zu speichernden Informationen zu reduzieren.

Datenfeld	Datentyp
Spalten (columns)	Array [0..n] von Tupel
OBIS-Kennzahl (obis)	String (obis)
Einheit (unit)	String (0..5)
Messwertliste (meterReadings)	Array [0..n] von Tupel
Zeitstempel (ts)	String (date-time)
Messwerte (values)	Array [0..n] von Number
Status der Messeinrichtung (meterStatus) (optional)	String (hexstring)
(verschiedene Status-Bezeichner)	

Tabelle 3.63 Beispiel: Kompakte Datenstruktur mit Spalten

Das folgende Pseudocode-Listing[21] zeigt die Verwendung des Datenfelds "Spalte" anhand der beispielhaften Messwertliste aus ▸Tabelle 3.63. Im Beispiel ist eine Anzahl von drei Spalten ("columns") definiert. In der Messwertliste sind Messwerte zu drei Zeitpunkten vorhanden ("meterReadings"). Es werden drei Messgrößen durch OBIS-Kennzahl ("obis") und Einheit ("unit") beschrieben. Die Zuordnung zwischen den Messwerten ("values" jeweils innerhalb jedes Tupels unter "meterReadings") und den Informationen in den Spalten ("columns") erfolgt positionsbasiert. Im Beispiel sind demnach die Werte "229.0", "228.0" und "231.0" der OBIS-Kennzahl "1-0:32.7.0" zugeordnet (analog "231.3", "227.3" und "233.3" zu "1-0:52.7.0" und so weiter).

```
{
   "columns" : [
      {
```

[21] Als Syntax wird hier JSON verwendet, ohne dass an dieser Stelle eine entsprechende Vorgabe gemacht wird.

```
            "obis":"1-0:32.7.0",
            "unit":"V"
         },
         {
            "obis":"1-0:52.7.0",
            "unit":"V"
         },
         {
            "obis":"1-0:72.7.0",
            "unit":"V"
         }
      ],
      "meterReadings":[
         {
            "ts":"2022-01-01T00:00:03Z",
            "values":[
               229.0,
               231.3,
               229.5
            ]
         },
         {
            "ts":"2022-01-01T00:00:13Z",
            "values":[
               228.0,
               227.3,
               0.0
            ],
            "meterStatus":{
               "phaseLoss":true
            }
         },
         {
            "ts":"2022-01-01T00:00:23Z",
            "values":[
               231.0,
               233.3,
               230.5
            ]
         }
      ]
   }
```


3.22.4 Abgeleiteter Wert und Liste abgeleiteter Werte (AWL)

Der Begriff "abgeleiteter Wert" beschreibt die Datenstruktur, die im Rahmen der Messwertverarbeitung einiger Tarifanwendungsfälle (▸FAKAT.ValProcBilling) auf Basis der ▸RWL gebildet werden. Die Datenstruktur ist in ▸Tabelle 3.64 beschrieben. Die Zuordnung zu einem Tarifanwendungsfall wird durch Persistierung innerhalb einer Liste abgeleiteter Werte (▸AWL) hergestellt.

3.22.4.1 Abgeleiteter Wert

Datenfeld	Datentyp	Beschreibung
Zeitstempel (ts)	String (dateTime)	Zeitpunkt, zu dem das Messwerttupel gebildet wurde. Die Semantik dieses Zeitpunkts ist abhängig vom verwendeten Tarifanwendungsfall: Für TAF2 und TAF8 der Endzeitpunkt des Abrechnungsturnus gemäß Auswertungsprofil.
Kombiniertes Statuswort (combinedStatus)	Tupel	Dieses Datenfeld enthält Statusinformationen. Hierin enthalten sind die Gerätestatusinformationen der Messeinrichtung und des SMGW. Folgende Elemente sind an dieser Stelle möglich: • CombinedStatus (definiert in ▸Tabelle 3.74)

Datenfeld	Datentyp	Beschreibung
Messwerte (values)	Array [0..n] von Tupel	Der Inhalt der Register zum Zeitpunkt "ts" Die Anzahl "n" der Register ist durch die Versandmesswerte-Konfiguration des Auswertungsprofiles und "tafType" bestimmt
Letzte Register-Aktualisierung (updateTs) (optional)	String (dateTime)	Dieses Datenfeld ist abhängig vom TAF vorhanden Letzte Aktualisierung des abgeleiteten Werteregisters
OBIS-ID (obis)	String (obis)	OBIS-ID des Messwertes
Messwert (value)	Number	Wert des Messwertes
Einheit (unit)	String (0..5)	Einheit des Messwertes (z.B. kWh)

Tabelle 3.64 Datenfelder des Datenobjekts "Abgeleiteter Wert" (derivedValue)

3.22.4.2 AWL

Datenfeld	Datentyp	Beschreibung
Messgeräteidentifikation (meterId)	String (huid)	Dieses Datenfeld enthält die herstellerübergreifende Identifikationsnummer der Messeinrichtung, deren registrierte Werte zur Ableitung verwendet wurden.
TAF-Typ (tafType)	Enumeration • TAF2 • TAF8	Der TAF-Typ definiert die Bedeutung der Zeitstempel und die Record-Typen der folgenden abgeleiteten Wertliste
Werteliste (recordList)	Array [0..n] von Tupel	Die Messwertsätze für den Abrechnungsturnus
Ein Messwertsatz Folgende Elemente sind an dieser Stelle möglich: • DerivedValue (definiert in ▸Tabelle 3.64)		

Tabelle 3.65 Datenfelder des Datenobjekts "Abgeleitete Werteliste (AWL)" (derivedValueList)

3.22.5 Eingangsmesswerte

Der Begriff "Eingangsmesswerte" beschreibt die Semantik der Daten, die von einer Messeinrichtung geliefert werden und vom SMGW verarbeitet werden. Dabei soll von den syntaktischen Datenstrukturen verschiedener Zählerprotokolle abstrahiert werden. Eingangsmesswerte sind beispielsweise Momentanwerte oder (akkumulierte) Zählerstände von Messgrößen, die in einer Messeinrichtung zeitgestempelt wurden, oder erst vom SMGW zeitgestempelt werden.

Die nachfolgende Tabelle beschreibt Mindestanforderungen an die Existenz und Granularität der Datenfelder der Eingangsmesswerte. Bei Empfang einer Messwertzulieferung erfolgt grundsätzlich eine Zeitstempelung. Werden die Eingangsmesswerte für einen abrechnungsrelevanten TAF verwendet, erfolgt weiterhin eine Validierung und Registrierung. Dabei werden die Eingangsmesswerte in eine Datenstruktur "registrierter Wert" überführt und in der zugehörigen Registrieren Wertliste (RWL) persistiert. Werden Eingangsmesswerte für einen nicht-abrechnungsrelevanten TAF verwendet, erfolgt die direkte Verarbeitung durch den TAF und temporäre Speicherung in der NWL.

Die Umwandlung protokollspezifischer Parameter der jeweiligen Messeinrichtung in die hier beschriebene Datenstruktur wird in den Detailspezifikationen für drahtlose und bedrahtete LMN-Protokolle beschrieben.

Der MSB gewährleistet vor der kommunikative Anbindung der Messeinrichtungen und im Betrieb, dass diese gemäß [MessEG]/[MessEV] zur Abrechnung verwendet werden dürfen.

Die Zeitpunkte zwischen Messung und Erfassung werden wie folgt differenziert:

1. Messzeitpunkt bzw. Zeitstempel der Messeinrichtung: Der Zeitpunkt, an dem ein Messwert in der Messeinrichtung gebildet wurde.
2. Sendezeitpunkt: Der Zeitpunkt, an dem eine Messwertnachricht aus der Messwerteinrichtung versandt wurde.
3. Empfangszeitpunkt: Der Zeitpunkt, an dem eine Messwertnachricht im SMGW empfangen wurde (Die Latenz zwischen Empfangszeitpunkt und Sendezeitpunkt wird durch die Kommunikation, Ver-/Entschlüsselung und Übertragungsstrecke bestimmt).
4. Sollregistrierzeitpunkt: Der gemäß Registrierperiode vorgegebene Zeitpunkt zu dem ein Messwert für die Abrechnung im SMGW gebildet wird (z.B. :00, :15, :30, :45 Minuten).

Datenfeld	Datentyp	Beschreibung
Messgeräteidentifikation (meterId)	String (huid)	Dieses Datenfeld enthält die herstellerübergreifende Identifikationsnummer der Messeinrichtung, die Ursprung dieser Messwertzulieferung ist.
Zeitstempel des Messwerts (ts)	String (dateTime)	Dieses Datenfeld enthält den vom SMGW bestimmten Messzeitpunkt bzw. den Versandzeitpunkt der Messwerte aus der Messeinrichtung. Wie der Messzeitpunkt oder Versandzeitpunkt vom SMGW bestimmt werden, ist abhängig vom verwendeten Protokoll der Messeinrichtung. Der Wert wird vom SMGW im Rahmen des Messwertempfangs bestimmt.
UTC Zeitstempel der Messeinrichtung (measurementTs) (optional)	String (dateTime)	Dieses optionale Datenfeld ist nur vorhanden, wenn die Messeinrichtung einen UTC Zeitstempel zum Messwert liefert. Dieses Datenfeld enthält den mit Informationen der Messeinrichtung bestimmten Messzeitpunkt für die übermittelten Messwerte.
Empfangszeitpunkt im SMGW (receiveTs)	String (dateTime)	Dieses Datenfeld enthält den vom SMGW im Rahmen des Messwertempfangs eingetragenen Empfangszeitpunkt der Messwertnachricht.
Messwerte (meterReadings)	Array [0..n] von Tupel	Dieses Datenfeld enthält eine Menge von Messwerten.
Messwert (value)	Number	Dieses Datenfeld enthält einen einzelnen Messwert.
OBIS-Kennzahl (obis)	String (obis)	Dieses Datenfeld identifiziert das Medium, die Messgröße und die Messart des zugehörigen Messwerts. Hierbei wird angenommen, dass eine gegebenenfalls notwendige Übersetzung in OBIS-Kennzahlen durch das SMGW bereits erfolgt ist (siehe Identifikation der Messgrößen in [DS] Kapitel "Wireless M-Bus Protokoll" und Kapitel "SML").
Einheit (unit)	String (0..5)	Dieses Datenfeld beschreibt die Einheit des Messwerts. Der zu verwendende Wert ist abhängig von der oben angegebenen OBIS-Kennzahl. Siehe auch ▸Abschnitt 2.5.2.
Status der Messeinrichtung (meterStatus) (optional)	Tupel	Dieses optionale Datenfeld kann entfallen, wenn der Status der Messeinrichtung ungestört und fehlerfrei ist. Das Datenfeld enthält in den Unterdatenfeldern verschiedene von der Messeinrichtung gelieferte Statusinformationen.
Hier findet sich die Statusinformationen der Messeinrichtung. Folgende Elemente sind an dieser Stelle möglich: • MeterStatus (definiert in ▸Tabelle 3.91)		

Tabelle 3.66 Datenfelder des Datenobjekts "Eingangsmesswerte" (acquisitionData)

3.22.6 Auswertungsprofil

Ein Auswertungsprofil enthält die notwendigen Datenfelder für den Betrieb eines Tarifanwendungsfalls (TAF). Die unten dargestellten Zwischenüberschriften dienen der Einteilung der Datenfelder nach ihrem Verwendungszweck und dienen nur der Lesbarkeit.

Parameter	Datentyp	Beschreibung
Profil-ID (profileId)	String (name)	Dieses Datenfeld identifiziert das Auswertungsprofil unter allen Auswertungsprofilen an den Schnittstellen des SMGW eindeutig. Dieses Datenfeld dient als Ressourcen-Identifikation.
Gültigkeitszeitraum (validityPeriod)	Tupel	Dieser Parameter legt den Zeitraum fest, für den der TAF im SMGW aktiv sein soll. Sofern das Auswertungsprofil auf einer Registrierperiode (Datenfeld "regInterval") basiert, stimmen Beginn und Ende des Gültigkeitszeitraumes mit einem Sollregistrierzeitpunkt überein.
Beginn (from)	String (dateTime)	Dieser Parameter legt den Beginn des Gültigkeitszeitraums fest.
Ende (to) (optional)	String (dateTime)	Wird dieser optionale Parameter nicht angegeben, dann wird von einem unendlich weit in der Zukunft liegenden Zeitpunkt ausgegangen, sodass der TAF nie beendet wird. Dieser Parameter legt das Ende des Gültigkeitszeitraums fest.
Parameter zur Konfiguration der Eingabe		
Zu verarbeitende Messgrößen (meterReadingInput)	Tupel	Dieser Parameter legt fest, welche erfassten Eingangsgrößen als Messwerte von welcher Messeinrichtung für die Verarbeitung innerhalb des TAF verwendet werden sollen. Eingabewerte können dabei pro Auswertungsprofil ausschließlich von genau einer Messeinrichtung verarbeitet werden. Er setzt sich zusammen aus den nachfolgenden Parametern.
Zugeordnetes LMN-Kommunikationsprofil (meterId)	String (huid)	Dieser Parameter referenziert ein LMN-Kommunikationsprofil anhand seiner eindeutigen Geräte-ID (meterId).
OBIS-Kennzahlen der zu verwendenden Messgrößen (obis)	Array [1..n] von String (obis)	Dieser Parameter definiert die Eingabegrößen der per LMN-Kommunikationsprofil angebundenen Messeinrichtung, die im Rahmen des TAF verwendet werden sollen.
Wandlerfaktor I (currentTransformerRatio) (optional)	Integer (1..60000)	Ist dieses Datenfeld nicht vorhanden, ist kein Wandler vorhanden bzw. der Wandlerfaktor ist 1.0 Dieses Datenfeld kann nur über das LMN-Kommunikationsprofil verändert werden. Dieser optionale Parameter wird nur ausgegeben, wenn die Messeinrichtung mit einem Messwandler für den Strompfad betrieben wird. Dieser Parameter enthält den Faktor des Messwandlers für den Strompfad I. Beispiel: Ein Wert 20.0 bedeutet, dass der Wandler einen Strom von 100A zu einem Strom von 5A an der Messeinrichtung umsetzt. Der Parameter wird nicht zur Berechnung im SMGW verwendet. Er wird vom MSB zur Verwendung durch den Anschlussnutzer/Anlagenbetreiber bereitgestellt.

Parameter	Datentyp	Beschreibung
Wandlerfaktor U (voltageTransformerRatio) (optional)	Integer (1..60000)	Ist dieses Datenfeld nicht vorhanden, ist kein Wandler vorhanden bzw. der Wandlerfaktor ist 1.0 Dieses Datenfeld kann nur über das LMN-Kommunikationsprofil verändert werden. Dieser optionale Parameter wird nur ausgegeben, wenn die Messeinrichtung mit einem Messwandler für den Spannungspfad betrieben wird. Dieser Parameter enthält den Faktor des Messwandlers für den Spannungspfad U. Beispiel: Ein Wert 100.0 bedeutet, dass der Wandler eine Spannung von 10.000V zu einer Spannung von 100V an der Messeinrichtung umsetzt. Der Parameter wird nicht zur Berechnung im SMGW verwendet. Er wird vom MSB zur Verwendung durch den Anschlussnutzer/Anlagenbetreiber bereitgestellt.
Parameter zur Konfiguration der Verarbeitung		
Auswahl des TAF (tafType)	Enumeration • TAF1 • TAF2 • TAF7 • TAF8 • TAF9 • TAF10 • TAF14 • TAF15	Dieser Parameter legt den Typ des Anwendungsfalls fest. Zulässig sind Bezeichner beginnend mit TAF, gefolgt von einer Zahl 1-99. Zulässige TAF-Typen und ihre Bedeutung werden in dieser TR oder einem Implementierungshinweis zur TR festgelegt.
TAF1 Parameter (taf1Params) (optional)	Tupel	Dieser Parameter ist nur für einen TAF1 vorhanden. Dieser Parameter legt die durchzuführende Verarbeitung im Rahmen des TAF fest. Ein Abrechnungsturnus wird nicht explizit angegeben, sondern es wird von einem monatlichen Abrechnungsturnus ausgegangen. Anhand der dabei versandten Daten kann auch eine jährliche Abrechnung vorgenommen werden. Das Ende jedes Abrechnungsturnus fällt auf den letzten Sollregistrierzeitpunkt bzw. das Tagesende jeden Monats. Ausnahme hiervon ist das Ende des Gültigkeitszeitraums, wo der letzte Zeitpunkt des Abrechnungsturnus auf den letzten Sollregistrierzeitpunkt bzw. Tagesende innerhalb des Gültigkeitszeitraums fällt.
Registrierperiode (regInterval)	Enumeration • FIVE_MINUTE • QUARTER_HOURLY • HOURLY • DAILY	Der Parameter legt den zeitliche Abstand zwischen zwei aufeinanderfolgenden registrierten Werten bzw. die tägliche Erfassung fest. Die Wertebelegungen haben folgende Bedeutung: • FIVE_MINUTE: 5 minütliche Registrierung zur Verwendung bei Lastgängen. • QUARTER_HOURLY: Viertelstündliche Registrierung zur Verwendung bei elektrischer Energie. • HOURLY: Stündliche Registrierung zur Verwendung bei Gas. • DAILY: Tägliche Registrierung zur Verwendung bei anderen Medien.
Tagesende (endOfDay) (optional)	Integer (0..23)	Sofern dieser optionale Parameter nicht angegeben ist, wird für elektrische Energie 0 bzw. 24 Uhr und für Gas 6 Uhr angenommen. Dieser Parameter legt für tägliche Registrierung, die Vorhaltung von Messwerten für den Bedarfsfall und die Erfassung von Tageswerten zur Verbrauchsinformation die Stunde des Tageswechsels fest.

Parameter	Datentyp	Beschreibung
Verwendbarkeit Abrechnung (validatedForBilling) (optional)	Boolean	Ist dieser optionale Parameter nicht vorhanden, wird der Standardwert angenommen. (Standardwert: true) Mithilfe dieses Parameters können Messwerte, die im Rahmen dieses TAF erhoben werden, als nicht für die Abrechnung verwendbar markiert werden (Paramterwert "false"). Ansonsten erfolgt keine solche Markierung. Der Parameter setzt dabei lediglich das Bit 1 im Statuswort der hierbei registrierten Messwerte auf "1". Die weitere Validierung und Verarbeitung der Messwerte erfolgt darüber hinaus unverändert.
TAF2 Parameter (taf2Params) (optional)	Tupel	Dieser Parameter ist nur für einen TAF2 vorhanden. Dieser Parameter legt die durchzuführende Verarbeitung im Rahmen des TAF fest.
Registrierperiode (regInterval)	Enumeration • FIVE_MINUTE • QUARTER_HOURLY • HOURLY	Der Parameter legt den zeitliche Abstand zwischen zwei aufeinanderfolgenden registrierten Werten fest. Die Wertebelegungen haben folgende Bedeutung: • FIVE_MINUTE: 5 minütliche Registrierung. • QUARTER_HOURLY: Viertelstündliche Registrierung. • HOURLY: Stündliche Registrierung.
Abrechnungsturnus (billingInterval)	Enumeration • MONTHLY • QUARTERLY • YEARLY	Dieser Parameter legt fest, in welchem Intervall die aktuellen Registerstände als neuer Wert in die AWL persistiert werden sollen. Die Wertebelegungen haben folgende Bedeutung: • MONTHLY: Monatlich zum Ersten des Monats. • QUARTERLY: Quartalsweise zum Ersten des Quartals. • YEARLY: Jährlich zum ersten des Jahres.
Zählzeitdefinition (timeOfUseDefinition) (optional)	Array [1..100000] von Tupel	Dieser Parameter muss gesetzt sein, wenn switchTimetable nicht gesetzt ist. Wenn switchTimetable gesetzt ist, muss dieser Parameter abwesend sein. Dieser Parameter definiert anhand von Paaren aus OBIS-Kennzahlen und Zeitpunkten lückenlos das jeweils aktive Register. Das aktive Register wird als Zielregister für die Kumulierung von Energiemengen verwendet. Zu jedem Zeitpunkt ist nur genau ein Register aktiv. Es ist nicht notwendig, für jeden Sollregistrierzeitpunkt ein Zielregister anzugegeben. Ein Wechsel des aktiven Registers erfolgt immer nur anhand eines hier konfigurierten Paares aus OBIS-Kennzahl und Zeitpunkt. Liegt für einen Sollregistrierzeitpunkt kein solches Paar vor, bleibt das bisher aktive Register weiterhin aktiv. Die Bedeutung der Zählzeitdefinition entspricht dem Universalbestellprozess der Energiemarktkommunikation (siehe GPKE).
Zu verwendende Tarifstufe (tariffNumber)	Integer (1..62)	Dieser Parameter legt fest, in welches Register Energiemengen ab dem angegebenen Zeitpunkt kumuliert werden sollen. Der Parameter gibt lediglich den Wert für die OBIS Wertegruppe "E" des abgeleiteten Registers an. Die OBIS-Kennzahl des abgeleiteten Registers bildet sich aus meterReadingInput.obis und dem Wert dieses Parameters.
Zeitpunkt (time)	String (dateTime)	Dieser Parameter definiert den Zeitpunkt, zu dem das per OBIS-Kennzahl definierte Register aktiv werden soll und damit als Zielregister für die Kumulierung von Energiemengen verwendet wird. Der angegebene Zeitpunkt muss auf einen Sollregistrierzeitpunkt gemäß der festgelegten Registrierperiode fallen.

Parameter	Datentyp	Beschreibung
Umschaltzeitplan (switchTimetable) (optional)	Tupel	Dieser Parameter muss gesetzt sein, wenn timeOfUseDefinition nicht gesetzt ist. Wenn timeOfUseDefinition gesetzt ist, muss dieser Parameter abwesend sein. Dieser Parameter definiert anhand von Zeitplänen das jeweils aktive Register. Das aktive Register wird als Zielregister für die Kumulierung von Energiemengen verwendet. Zu jedem Zeitpunkt ist nur genau ein Register aktiv.
Saisonzeitpläne (seasonTables)	Array [1..n] von Tupel	Die Saisonzeitpläne legen anhand eines Startdatums den ab diesem Zeitpunkt zu verwendenden Wochenzeitplan fest. Die Liste der Saisonzeitpläne sind nach Startdatum sortiert. Wird der Startzeitpunkt des nächsten Saisonzeitplans erreicht, gilt dessen Festlegung des zu verwendenden Wochenzeitplan und löst die bisher bestehende Festlegung des Wochenzeitplans ab.
Name (name)	String (0..255)	Ein innerhalb dieses Auswertungsprofils eindeutiger Name zur Identifikation des Saisonzeitplans.
Startdatum (start)	String (dateTime)	Legt das Startdatum fest, zu dem dieser Saisonzeitplan zu verwenden ist.
Wochenzeitpläne (weekTables)	Array [1..n] von Tupel	Die Wochenzeitpläne legen für die verschiedenen Wochentage den jeweils zu verwendenden Tageszeitplan fest.
Name (name)	String (0..255)	Ein innerhalb dieses Auswertungsprofils eindeutiger Name zur Identifikation des Wochenzeitplans.
Montag (monday) (optional)	Integer (0..65535)	Ist dieser Parameter nicht vorhanden, findet keine Änderung der Festlegung des Tageszeitplans zu diesem Wochentag statt. Dieser Parameter legt den zu verwendenden Tageszeitplan anhand seiner Identifikation (dayId) für Montage fest.
Dienstag (tuesday) (optional)	Integer (0..65535)	Ist dieser Parameter nicht vorhanden, findet keine Änderung der Festlegung des Tageszeitplans zu diesem Wochentag statt. Dieser Parameter legt den zu verwendenden Tageszeitplan anhand seiner Identifikation (dayId) für Dienstage fest.
Mittwoch (wednesday) (optional)	Integer (0..65535)	Ist dieser Parameter nicht vorhanden, findet keine Änderung der Festlegung des Tageszeitplans zu diesem Wochentag statt. Dieser Parameter legt den zu verwendenden Tageszeitplan anhand seiner Identifikation (dayId) für Mittwoche fest.
Donnerstag (thursday) (optional)	Integer (0..65535)	Ist dieser Parameter nicht vorhanden, findet keine Änderung der Festlegung des Tageszeitplans zu diesem Wochentag statt. Dieser Parameter legt den zu verwendenden Tageszeitplan anhand seiner Identifikation (dayId) für Donnerstage fest.
Freitag (friday) (optional)	Integer (0..65535)	Ist dieser Parameter nicht vorhanden, findet keine Änderung der Festlegung des Tageszeitplans zu diesem Wochentag statt. Dieser Parameter legt den zu verwendenden Tageszeitplan anhand seiner Identifikation (dayId) für Freitage fest.
Samstag (saturday) (optional)	Integer (0..65535)	Ist dieser Parameter nicht vorhanden, findet keine Änderung der Festlegung des Tageszeitplans zu diesem Wochentag statt. Dieser Parameter legt den zu verwendenden Tageszeitplan anhand seiner Identifikation (dayId) für Samstage fest.
Sonntag (sunday) (optional)	Integer (0..65535)	Ist dieser Parameter nicht vorhanden, findet keine Änderung der Festlegung des Tageszeitplans zu diesem Wochentag statt. Dieser Parameter legt den zu verwendenden Tageszeitplan anhand seiner Identifikation (dayId) für Sonntage fest.

Parameter	Datentyp	Beschreibung
Tagespläne (dayTables)	Array [0..n] von Tupel	Die Tagespläne legen für einen Tag den jeweils zu verwendenden Tageszeitplan fest.
Tagesplanidentifikation (dayId)	Integer (0..65535)	Dieser Parameter identifiziert das Tagesprofil innerhalb dieses Auswertungsprofils eindeutig.
Tageszeitpläne (daytimeTables)	Array [0..n] von Tupel	Dieser Parameter enthält die an einem Tag anzuwendenen Tarifumschaltzeitpunkte und zu verwendende Tarifstufe.
Startzeit (startTime)	Tupel	Dieser Parameter legt den Zeitpunkt fest, an dem das via tariffNumber angegebene Register aktiv werden soll.
Stunde (hour) (optional)	Integer (0..23)	Ist dieser Parameter nicht vorhanden, wird er als Wildcard interpretiert ("jede Stunde"). Legt die Stunde fest.
Minute (minute) (optional)	Integer (0..59)	Ist dieser Parameter nicht vorhanden, wird er als Wildcard interpretiert ("jede Minute"). Legt die Minute fest.
Tarifstufe (tariffNumber) (optional)	Integer (1..62)	Ist dieser Parameter nicht vorhanden, findet keine Änderung der aktiven Tarifstufe statt. Dieser Parameter legt fest, in welches Register Energiemengen ab dem angegebenen Zeitpunkt kumuliert werden sollen. Der Parameter gibt lediglich den Wert für die OBIS Wertegruppe "E" des abgeleiteten Registers an. Die OBIS-Kennzahl des abgeleiteten Registers bildet sich aus meterReadingInput.obis und dem Wert dieses Parameters. Das über diesen Parameter festgelegte Register löst zum Umschaltzeitpunkt (startTime) das bisher aktive Register ab. Energiemengen werden immer nur in genau das eine aktive Register kumuliert.
Preisstufen (cost) (optional)	Array [1..63] von Tupel	Ist dieser optionale Parameter nicht vorhanden, werden keine Informationen an den Anschlussnutzer bereitgestellt. Dieser Parameter erlaubt das Hinterlegen von Preisbestandteilen für die verschiedenen Register. Sofern die Information hinterlegt ist, kann sie an Geräte des Anschlussnutzers (beispielsweise EMS) weitergegeben werden. Dies fördert ein anreizbasiertes Verhalten des Anschlussnutzers im Hinblick auf EU Richtlinie 2019/944.
Tarifstufe (tariffNumber)	Integer (1..62)	Dieser Parameter legt fest, für welche Tarifstufe (angegeben als Werte für Wertegruppe "E" für die abgeleiteten Register auf Basis von meterReadingInput.obis) die angegebenen Preisbestandteile anwendbar ist.
Preisbestandteile (priceComponents)	Tupel	Dieser Parameter enthält einen oder mehrere Preisbestandteile.
Name des Preisbestandteil (name)	String (1..32)	Name des Preisbestandteils einschließlich Hinweis auf brutto bzw. netto.
Preis des Preisbestandteils (amount)	Number	Der aufgerufene Preis für den benannten Preisbestandteil in Cent.
Tagesende (endOfDay) (optional)	Integer (0..23)	Sofern dieser optionale Parameter nicht angegeben ist, wird für elektrische Energie 0 bzw. 24 Uhr und für Gas 6 Uhr angenommen. Dieser Parameter legt für die Vorhaltung von Messwerten für den Bedarfsfall und die Erfassung von Tageswerten zur Verbrauchsinformation die Stunde des Tageswechsels fest.

Parameter	Datentyp	Beschreibung
Verwendbarkeit Abrechnung (validatedForBilling) (optional)	Boolean	Ist dieser optionale Parameter nicht vorhanden, wird der Standardwert angenommen. (Standardwert: true) Mithilfe dieses Parameters können Messwerte, die im Rahmen dieses TAF erhoben werden, als nicht für die Abrechnung verwendbar markiert werden (Paramterwert "false"). Ansonsten erfolgt keine solche Markierung. Der Parameter setzt dabei lediglich das Bit 1 im Statuswort der hierbei registrierten Messwerte und der abgeleiteten Werte auf "1". Die weitere Validerung und Verarbeitung der Messwerte erfolgt darüber hinaus unverändert.
TAF7 Parameter (taf7Params) (optional)	Tupel	Dieser Parameter ist nur für einen TAF7 vorhanden. Dieser Parameter legt die durchzuführende Verarbeitung im Rahmen des TAF fest.
Registrierperiode (regInterval)	Enumeration • FIVE_MINUTE • QUARTER_HOURLY • HOURLY	Der Parameter legt den zeitliche Abstand zwischen zwei aufeinanderfolgenden Registrierten Werten fest. Die Wertebelegungen haben folgende Bedeutung: • FIVE_MINUTE: 5 minütliche Registrierung. • QUARTER_HOURLY: Viertelstündliche Registrierung. • HOURLY: Stündliche Registrierung.
Abrechnungsturnus (billingInterval)	Enumeration • DAILY • MONTHLY	Dieser Parameter definiert über welchen Zeitraum registrierte Werte für den Messwertversand zusammengefasst werden sollen. Dies ist nicht zu verwechseln mit dem Versandzeitpunkt. Die Wertebelegungen haben folgende Bedeutung: • DAILY: tägliche Zusammenfassung um Mitternacht. • MONTHLY: monatliche Zusammenfassung zum letzten Sollregistrierzeitpunkt des Monats.
Tagesende (endOfDay) (optional)	Integer (0..23)	Sofern dieser optionale Parameter nicht angegeben ist, wird für elektrische Energie 0 bzw. 24 Uhr und für Gas 6 Uhr angenommen. Dieser Parameter legt für die Vorhaltung von Messwerten für den Bedarfsfall und die Erfassung von Tageswerten zur Verbrauchsinformation die Stunde des Tageswechsels fest.
Verwendbarkeit Abrechnung (validatedForBilling) (optional)	Boolean	Ist dieser optionale Parameter nicht vorhanden, wird der Standardwert angenommen. (Standardwert: true) Mithilfe dieses Parameters können Messwerte, die im Rahmen dieses TAF erhoben werden, als nicht für die Abrechnung verwendbar markiert werden (Paramterwert "false"). Ansonsten erfolgt keine solche Markierung. Der Parameter setzt dabei lediglich das Bit 1 im Statuswort der hierbei registrierten Messwerte auf "1". Die weitere Validerung und Verarbeitung der Messwerte erfolgt darüber hinaus unverändert.
TAF8 Parameter (taf8Params) (optional)	Tupel	Dieser Parameter ist nur für einen TAF8 vorhanden. Dieser Parameter legt die durchzuführende Verarbeitung im Rahmen des TAF fest.
Registrierperiode (regInterval)	Enumeration • FIVE_MINUTE • QUARTER_HOURLY • HOURLY	Der Parameter legt den zeitlichen Abstand zwischen zwei aufeinanderfolgenden registrierten Werten fest. Die Wertebelegungen haben folgende Bedeutung: • FIVE_MINUTE: 5 minütliche Registrierung. • QUARTER_HOURLY: Viertelstündliche Registrierung. • HOURLY: Stündliche Registrierung.

Parameter	Datentyp	Beschreibung
Abrechnungsturnus (reportingPeriod)	Enumeration • DAILY • MONTHLY	Dieser Parameter definiert, über welchen Zeitraum abgeleitete Werte für den Messwertversand zusammengefasst werden sollen. Dies ist nicht zu verwechseln mit dem Versandzeitpunkt. Der Leistungsmaximalwert wird innerhalb des parametrierten Abrechnungsturnus unter Verwendung der Messperiode bestimmt. Die Wertebelegungen haben folgende Bedeutung: • DAILY: Der Abrechnungsturnus umfasst einen Tag. Die Zusammenfassung geschieht nach Ablauf des Akzeptanzfensters des letzten Sollregistrierzeitpunktes des laufenden Tages. • MONTHLY: Der Abrechnungsturnus umfasst einen Monat. Die Zusammenfassung geschieht nach Ablauf des Akzeptanzfensters des letzten Sollregistrierzeitpunktes des laufenden Monats.
Tagesende (endOfDay) (optional)	Integer (0..23)	Sofern dieser optionale Parameter nicht angegeben ist, wird für elektrische Energie 0 bzw. 24 Uhr und für Gas 6 Uhr angenommen. Dieser Parameter legt für die Vorhaltung von Messwerten für den Bedarfsfall und die Erfassung von Tageswerten zur Verbrauchsinformation die Stunde des Tageswechsels fest.
Verwendbarkeit Abrechnung (validatedForBilling) (optional)	Boolean	Ist dieser optionale Parameter nicht vorhanden, wird der Standardwert angenommen. (Standardwert: true) Mithilfe dieses Parameters können Messwerte, die im Rahmen dieses TAF erhoben werden, als nicht für die Abrechnung verwendbar markiert werden (Paramterwert "false"). Ansonsten erfolgt keine solche Markierung. Der Parameter setzt dabei lediglich das Bit 1 im Statuswort der hierbei registrierten Messwerte auf "1". Die weitere Validerung und Verarbeitung der Messwerte erfolgt darüber hinaus unverändert.
TAF9 Parameter (taf9Params) (optional)	Tupel	Dieser Parameter ist nur für einen TAF9 vorhanden. Dieser Parameter legt die durchzuführende Verarbeitung im Rahmen des TAF fest.
Erfassungsperiode (capPeriod)	Integer (1..86400)	Dieser Parameter legt den zeitlichen Abstand in Sekunden fest, in dem Messwerte für diesen TAF erfasst werden.
Wertaufbereitung (preprocessing) (optional)	Enumeration • Keine (NONE) • Vorzeichenkorrektur (SIGN_INVERT) • Verbrauchsnullung (CONSUMPTION_CAP)	Ist dieser optionale Parameter nicht vorhanden, wird der Standardwert angenommen. (Standardwert: NONE) Dieser Parameter definiert, wie eingehende Messwerte anhand ihrer OBIS-Kennzahl datenschutzkonform zu verarbeiten sind. Die Wertebelegungen haben folgende Bedeutung: • Keine (NONE): es besteht keine Notwendigkeit einer Veränderung der Messwerte. • Vorzeichenkorrektur (SIGN_INVERT): entspricht das Vorzeichen der gelieferten Strom- und Leistungsmomentanwerte nicht der Vorgabe der OBIS-IDs dieser TR (negativ = Einspeisung, positiv = Verbrauch), beispielsweise bei Verwendung eines Einspeisezählers, wird bei dieser Auswahlmöglichkeit das Vorzeichen vom SMGW korrigiert. • Verbrauchsnullung (CONSUMPTION_CAP): bei Verwendung eines Zweirichtungszählers, der Strom- und Leistungsmomentanwerte in Abhängigkeit der Richtung mit Vorzeichen versieht (negativ = Einspeisung, positiv = Verbrauch). Hierbei sollen positive und damit personenbeziehbare Verbrauchswerte als Nullwert angenommen werden.
TAF10 Parameter (taf10Params) (optional)	Tupel	Dieser Parameter ist nur für einen TAF10 vorhanden. Dieser Parameter legt die durchzuführende Verarbeitung im Rahmen des TAF fest.
Erfassungsperiode (capPeriod)	Integer (1..86400)	Dieser Parameter legt den zeitlichen Abstand in Sekunden fest, in dem Messwerte für diesen TAF erfasst werden.

Parameter	Datentyp	Beschreibung
Pseudonym (pseudonym) (optional)	String (8..64)	Ist dieser optionale Parameter vorhanden, wird die meterId beim Versand durch den Inhalt dieses Datenfeldes ersetzt. Dieses Datenfeld enthält das vom GWA so gewählte Pseudonym für die Messeinrichtung, dass der EMT anhand des Pseudonyms keinen Bezug zur Messlokation herstellen kann.
TAF14 Parameter (taf14Params) (optional)	Tupel	Dieser Parameter ist nur für einen TAF14 vorhanden. Dieser Parameter legt die durchzuführende Verarbeitung im Rahmen des TAF fest.
Erfassungsperiode (capPeriod)	Integer (1..86400)	Dieser Parameter legt den zeitlichen Abstand in Sekunden fest, in dem Messwerte für diesen TAF erfasst werden.
TAF15 Parameter (taf15Params) (optional)	Tupel	Dieser Parameter ist nur für einen TAF15 vorhanden. Dieser Parameter legt die durchzuführende Verarbeitung im Rahmen des TAF fest.
Erwartete Registrierperiode (regInterval)	Enumeration • FIVE_MINUTE • QUARTER_HOURLY • HOURLY	Der Parameter legt den zeitlichen Abstand zwischen zwei aufeinanderfolgenden registrierten Werten aus der Messeinrichtung fest. Die Wertebelegungen haben folgende Bedeutung: • FIVE_MINUTE: 5 minütliche Registrierung. • QUARTER_HOURLY: Viertelstündliche Registrierung. • HOURLY: Stündliche Registrierung.
Abrechnugsturnus (billingInterval)	Enumeration • DAILY • MONTHLY • HOURLY • QUARTER_HOURLY	Dieser Parameter definiert über welchen Zeitraum registrierte Werte für den Messwertversand zusammengefasst werden sollen. Dies ist nicht zu verwechseln mit dem Versandzeitpunkt. Die Wertebelegungen haben folgende Bedeutung: • DAILY: Der Abrechnugsturnus umfasst einen Tag. Die Zusammenfassung geschieht nach Ablauf des Akzeptanzfensters des letzten Sollregistrierzeitpunktes des laufenden Tages. • MONTHLY: Der Abrechnugsturnus umfasst einen Monat. Die Zusammenfassung geschieht nach Ablauf des Akzeptanzfensters des letzten Sollregistrierzeitpunktes des laufenden Monats. • HOURLY: Der Abrechnugsturnus umfasst einen Monat. Die Zusammenfassung geschieht nach Ablauf des Akzeptanzfensters des letzten Sollregistrierzeitpunktes der laufenden Stunde. • QUARTER_HOURLY: Der Abrechnugsturnus umfasst eine Viertelstunde. Die Zusammenfassung geschieht nach Ablauf des Akzeptanzfensters des letzten Sollregistrierzeitpunktes der laufenden Viertelstunde.
Tagesende (endOfDay) (optional)	Integer (0..23)	Sofern dieser optionale Parameter nicht angegeben ist, wird für elektrische Energie 0 bzw. 24 Uhr und für Gas 6 Uhr angenommen. Dieser Parameter legt für die Vorhaltung von Messwerten für den Bedarfsfall und die Erfassung von Tageswerten zur Verbrauchsinformation die Stunde des Tageswechsels fest.
Parameter zur Ausgabe im HAN		
Zuordneter Anschlussnutzer (userId)	String (name)	Dieser Parameter referenziert ein HAN-Kommunikationsprofil mit Rolle "CON" über die eindeutige Kennung des Anschlussnutzers (userId) und bestimmt darüber den Anschlussnutzer, der zur Einsicht der Daten berechtigt ist.
Zuordnete CLS (clsIds) (optional)	Array [1..10] von String (name)	Ist dieser optionale Parameter nicht vorhanden, kann kein CLS auf die dem Zähler/Auswertungsprofil zugeordneten Messwerte zugreifen. Dieser Parameter referenziert ein oder mehrere HAN-Kommunikationsprofile mit Rolle "CLS" jeweils über die eindeutige Kennung des CLS (userId im HAN-Kommunikationsprofil) und bestimmt darüber die CLS, die Messdaten erhalten dürfen.

Parameter	Datentyp	Beschreibung
Parameter zur Konfiguration der Ausgabe im WAN		
Zählpunktbezeichnung (meteringPointId)	String (name)	Dieser Parameter stellt den beim Export zu sendenden eindeutigen Bezeichner der Messlokation dar.
Identifikation des Marktpartners (mpId)	String (name)	Dieser Parameter enthält eine Identifikation des Marktpartners (Für den Strommarkt: Siehe bdew-codes.de). Der Marktpartner ist zu unterscheiden vom Empfänger der Messwerte (siehe "Zugeordnetes WAN-Kommunikationsprofil"), da dieser die Messwerte ggf. über einen Dritten erhält. Es dient dem Anschlussnutzer als Transparenzinformation für versandte Werte.
Anwendungsreferenz (tafId)	Tupel	Der Inhalt dieses Parameters wird beim Versand der Messwerte an den EMT übermittelt, damit der berechtigte Empfänger einen Bezug zwischen bestellter Konfiguration und zugelieferten Werten herstellen kann. Die Zuordnung der Identifikation zu Anschlussnutzern findet beim berechtigten Empfänger statt.
Identifikation des Marktpartners (mpId)	String (name)	Dieser Parameter enthält eine Identifikation des Marktpartners (Für den Strommarkt: Siehe bdew-codes.de). Der Marktpartner ist zu unterscheiden vom Empfänger der Messwerte (siehe "Zugeordnetes WAN-Kommunikationsprofil"), da dieser die Messwerte ggf. über einen Dritten erhält. Es dient dem Anschlussnutzer als Transparenzinformation für versandte Werte.
Zählpunktbezeichnung (meteringPointId)	String (name)	Dieser Parameter stellt den beim Export zu sendenden eindeutigen Bezeichner der Messlokation gemäß [VDE44400] dar.
Marktpartner-Rolle (mpRole)	String (name)	Dieser Parameter enthält die beim Export zu übermittelnde Rolle des Marktpartners gemäß [VDE4400].
MSB spezifisch (msbSpecific) (optional)	String (name)	Ist dieses Optionale Datenfeld nicht vorhanden, wird die Anwendungsreferenz mit "0" aufgefüllt. Dieser wird gemäß [VDE44400] vom MSB vergeben und dient ihm als Referenz zur Zuordnung der Versandten Messwerte.
Zu versendende Werte (meterDataOutput)	Tupel	Dieser Parameter legt fest, welche Werte ein berechtigter Empfänger erhalten sollen und durch welche Auslöser ein Versand eingeleitet wird.
OBIS-Kennzahlen der zu versendenden Messgrößen (obis)	Array [0..n] von String (obis)	Dieser Parameter legt fest, welche Werte an den berechtigten Empfänger versendet werden sollen. Die zu versendenden Werte wurden dabei im Rahmen der Verarbeitung innerhalb des TAF erzeugt.
Identifikation des WAN-Kommunikationsprofils (wanPeerRef)	String (1..64)	Dieser Parameter enthält eine Referenz auf ein WAN-Kommunikationsprofil vom Typ INFO-REPORT (profileId) als berechtigtem Empfänger für den die Messwert-Nachrichten verschlüsselt sind.
Über GWA (viaGwa) (optional)	Boolean	Sofern dieses optionale Parameter nicht vorhanden ist, wird der Standardwert angenommen. Wenn das SMGW die Funktion nicht unterstützt, muss der Parameter abwesend sein. (Standardwert: false) Legt fest, dass der Versand der Messwert-Nachrichten über den GWA, aber verschlüsselt für den EMT erfolgt. Die Nachrichten werden gemäß "wanPeerRef" EMT-WAN-Kommunikationsprofil (INFO-REPORT) verschlüsselt und mit den Kommunikationsparametern des GWA-WAN-Kommunikationsprofiles (ADMIN-SERVICE) an den GWA übermittelt. Siehe auch ▸ICS.FAKAT.ValTransmission.10.

Parameter	Datentyp	Beschreibung
Versandauslöser (trigger)	Tupel	Dieser Parameter bzw. die darin enthaltenen Parameter legen fest, zu welchem Auslöser ein Versand an den per "Zugeordnetes WAN-Kommunikationsprofil" festgelegten, berechtigten Empfänger erfolgen soll. Auslöser können auf verschiedene Weise definiert werden (zeitlich periodisch, bei Schwellwertverletzung, bei Ereignis). Es kann nur eine Art von Versandauslöser konfiguriert werden. Die Kombination mehrerer Auslöser ist nicht möglich. Ist für TAF9, TAF10 oder TAF14 kein Auslöser festgelegt, werden die Werte beim Eintreffen sofort versandt (Ad-hoc-Versand). Ein durch den GWA ausgelöster Versand im Bedarfsfall ist unabhängig von der hier festgelegten Parametrierung vorhanden, sofern dies vom jeweiligen TAF unterstützt wird.
Versandzeitpunkt (deliveryTime) (optional)	Tupel	Ist dieser optionale Parameter nicht vorhanden, erfolgt kein zeitlich periodischer Versand. Dieser Parameter definiert unter Angabe von Zeitkomponenten (Jahr, Monat, Tag des Monats, Stunde, Minute, Sekunde) periodische Versandzeitpunkte. Ist eine Zeitkomponente nicht vorhanden, wird diese als Wildcard angenommen so dass jeder Wert im Vergleich übereinstimmt. Sind alle Zeitkomponenten nicht vorhanden, entspricht dies einem minütlichen Versand zur vollen Minute.
Jahr (year) (optional)	Integer (2000..2100)	Ist dieser optionale Parameter nicht vorhanden, erfolgt der Versand in jedem Jahr. Dieser Parameter legt fest, in welchem Jahr ein Versand erfolgen soll.
Monat (month) (optional)	Integer (1..12)	Ist dieser optionale Parameter nicht vorhanden, erfolgt der Versand in jedem Monat. Dieser Parameter legt fest, in welchem Monat ein Versand erfolgen soll.
Tag des Monats (day) (optional)	Integer (1..31)	Ist dieser optionale Parameter nicht vorhanden, erfolgt der Versand an jedem Tag eines Monats. Dieser Parameter legt fest, an welchem Tag eines Monat ein Versand erfolgen soll.
Stunde (hour) (optional)	Integer (0..23)	Ist dieser optionale Parameter nicht vorhanden, erfolgt der Versand jede Stunde eines Tages. Dieser Parameter legt fest, zu welcher Stunde eines Tages ein Versand erfolgen soll.
Minute (minute) (optional)	Integer (0..59)	Ist dieser optionale Parameter nicht vorhanden, erfolgt der Versand jede Minute einer Stunde. Dieser Parameter legt fest, zu welcher Minute innerhalb einer Stunde ein Versand erfolgen soll.
Sekunde (second) (optional)	Integer (0..59)	Ist dieser optionale Parameter nicht vorhanden, wird die volle Minute angenommen. (Standardwert: 0) Dieser Parameter legt fest, zu welcher Sekunde innerhalb einer Minute ein Versand erfolgen soll.
Schwellwerte (thresholds) (optional)	Array [1..10] von Tupel	Dieser Parameter ist nur bei TAF9, TAF10 und TAF14 relevant. Ist er für TAF dieses Typs nicht vorhanden, erfolgt kein Versand auf Basis von Schwellwerten. Dieser Parameter erlaubt die Überwachung eines oder mehrerer Messwerte auf eine Schwellwertunter- oder -überschreitung. Sobald eine Schwellwertverletzung erkannt wird, wird ein Versand ausgelöst. Ein erneuter Versand erfolgt erst bei erneutem Auftreten einer Schwellwertverletzung, nachdem zuvor keine Schwellwertverletzung erkannt wurde.

Parameter	Datentyp	Beschreibung
OBIS-Kennzahl (obis)	String (obis)	Dieser Parameter legt fest, welche unter "Zu verarbeitende Messgrößen" definierte Messgröße für die Schwellwertüberwachung berücksichtigt werden soll.
Operation (operator)	Enumeration • Unterschreitung (FALLING) • Überschreitung (RISING)	Dieser Parameter legt die Richtung der Schwellwertüberwachung fest. Bei "Unterschreitung" wird eine Schwellwertverletzung erkannt, sobald der zu überwachende Messwert die festgelegte Schwelle unterschreitet.
Schwelle (threshold)	Number	Dieser Parameter legt die zu überwachende Schwelle fest.
Hysterese (hysteresis)	Number	Dieser Parameter legt eine Hysterese fest, um ungewünschten Mehrfachversand bei Schwellwertverletzung zu vermeiden. Wurde zuvor eine Schwellwertverletzung erkannt, dann muss der eingehende Messwert zunächst über den Hysteresewert steigen (bei Überwachung auf Unterschreitung) bzw. darunter fallen (bei Überwachung auf Überschreitung). Ist der Wert der Hysterese identisch zur Schwelle, entspricht dies einer Deaktivierung der Hysterese.
Signaturmodus (signMode) (optional)	Enumeration • Keine (NONE) • CMS_ECDSA_SHA256_detached	Ist dieser optionale Parameter nicht vorhanden, wird der Standardwert angenommen. (Standardwert: CMS_ECDSA_SHA256_detached) Dieser Parameter erlaubt die Einstellung der zu erstellenden Signatur beim Messwertversand. Die Wertebelegungen haben folgende Bedeutung: • Keine (NONE): es wird keine Signatur erstellt. • CMS_ECDSA_SHA256_detached: Verfahren zur Signierung mittels Signatur, die in die Exportdatenstruktur eingebettet wird.
TAF-Zustandsübergänge		
TAF-Zustand (tafState)	Enumeration • ready • running • archive	Dieser (Read-Only) Parameter stellt den aktuellen Zustand des TAFs bereit. Die Wertebelegungen haben folgende Bedeutung: • ready: Konfiguriert, aber Gültigkeit noch nicht begonnen. Messwerte liegen noch nicht vor. • running: Innerhalb des Gültigkeitszeitraumes. Messwertverarbeitung und -speicherung findet statt. • archive: Nach Gültigkeitsende. Messwertverarbeitung findet nicht statt. Konfiguration und Messwerte werden aufbewahrt.
Archivierungsdauer (archiveDuration)	Integer (0..9999)	Dieser Parameter legt die Archivierungsdauer des TAF und der zugehörigen Messwerte in Tagen fest. Bei Angabe von "0" endet die Archivierungsdauer unmittelbar nach Ende des Gültigkeitszeitraumes.
Automatisches Löschen (autoCleanUp) (optional)	Boolean	Ist dieser optionale Parameter nicht vorhanden, wird der Standardwert angenommen. (Standardwert: true) Dieser Parameter legt fest, ob das Auswertungsprofil und die im Gültigkeitszeitraum erfassten Messwerte automatisch vom SMGW nach Ablauf der Archivierungsdauer gelöscht werden sollen.

Tabelle 3.67 Parameter des Profils "Auswertungsprofil" (processingProfile)

3.22.7 AuthChallenge-Datenstrukturen

Datenstruktur für die Übermittlung einer "Challenge", die für die Authentifizierung benötigt wird.

Datenfeld	Datentyp	Beschreibung
Challenge (challenge)	String (hexString)	Dieses Datenfeld enthält die Zufallszahl (16 oder 32 Bytes), die in die Berechnung der AuthResponse einfließt.
Authentifizierungsalgorithmen (authAlgoList) (optional)	Array [0..3] von Enumeration • ECDSA_PLAIN_SHA256	Wird dieser optionale Parameter nicht angegeben wird der Default verwendet. (Standardwert: ecdsa-plain-SHA256) Das SMGW übermittelt dem Authentisierenden die Verfahren, die mit dem im SMGW gespeicherten Authentisierungsschlüssel verwendbar und implementiert sind. Das Verfahren ecdsa-plain-SHA256 ist in [TR-03111] beschrieben (ECDSA-Signatur r||s über den Hash SHA256(challenge)).

Tabelle 3.68 Datenfelder des Datenobjekts "AuthChallenge" (authChallenge)

3.22.8 AuthResponse-Datenstruktur

Datenstruktur für die Übermittlung eines signierten Tokens, das für die Authentifizierung benötigt wird.

Parameter	Datentyp	Beschreibung
Token (token)	String (hexString)	Dieses Datenfeld enthält die vom Authentisierenden signierten Daten, die validiert werden.
Hinweis auf Authentifizierungszertifikat (authCert) (optional)	String (hexString)	Ist dieses optionale Datenfeld nicht vorhanden, wird im SMGW der GW_WAN_AUT_PUB zum TLS-Zertifikat des GWA-Zertikatssatzes des aktuellen GWA-Schlüsselsatzes (Domäne "gwa") zur Validierung verwendet. Das Datenfeld enthält einen Hinweis auf das vom Authentisierenden gewählte TLS-Zertifikat, dessen öffentlicher Schlüssel GWA_WAN_TLS_PUB dem GWA_WAN_AUT_PUB entspricht. Dieses Datenfeld unterstützt im Falle einer überlappenden Gültigkeit eines GWA-Zertifikatssatzes (Wechselprozess oder Redundanz) die Auswahl des geeigneten Authentisierungsschlüssels für das Token
Authentifizierungsalgorithmus (authAlgo) (optional)	Enumeration • ECDSA_PLAIN_SHA256	Ist dieses optionale Datenfeld nicht vorhanden, bestimmt das SMGW anhand des für die Validierung verwendeten öffentlichen Schlüssels das Authentifizierungsverfahren. Das Datenfeld enthält das vom Authentisierenden gewählte Authentifizierungsverfahren (passend zum Signaturschlüssel, mit dem das Token signiert wurde).

Tabelle 3.69 Parameter des Profils "AuthChallenge" (authChallenge)

3.22.9 Benachrichtigungsprofil

Ein Benachrichtigungsprofil legt fest, über welche Ereignisse ein GWA benachrichtigt werden soll.

Jedes Ereignis-Tupel (vendor, eventId, eventSubId) darf nur einmal in der Liste vorkommen.

Die Bedeutung der Ereignistypen ist in ▸Anhang A beschrieben.

Parameter	Datentyp	Beschreibung
Profil-ID (profileId)	String (name)	Dieses Datenfeld identifiziert das Benachrichtigungsprofil unter allen Benachrichtigungsprofilen an den Schnittstellen des SMGW eindeutig. Dieses Datenfeld wird als Ressourcen-Identifikation verwendet.
Liste von Ereignissen zur Benachrichtigung (notificationEvents)	Array [0..n] von Tupel	Liste von Ereignissen, die zu einer Benachrichtigung des GWA führen.
Interessensträger (vendor)	String (3..3)	Dreistellige (Uppercase) Kennzeichnung des Interessensträgers
Ereignistyp (eventId)	Integer (0..65535)	Identifiziert den Ereignistyp.

Parameter	Datentyp	Beschreibung
Ereignisuntertyp (eventSubId)	Integer (0..65535)	Identifiziert den Ereignisuntertyp. 0 kennzeichnet ein positives (erfolgreiches) Ereignis.

Tabelle 3.70 Parameter des Profils "Benachrichtigungsprofil" (notificationProfile)

3.22.10 Zertifikat und Schlüssel

Diese Datenstruktur enthält einen privaten Schlüssel und das zugehörige Zertifikat als Ergebnis des Zertifikatserstellungsdienstes des SMGW.

Datenfeld	Datentyp	Beschreibung
Zertifikat (cert)	String (hexString)	Dieses Datenfeld enthält das gemäß [RFC5280] in ASN.1 gemäß [X.690] DER codierte X.509 Zertifikat zum privaten Schlüssel des Datenfeldes "privateKey".
Privater Schlüssel (privateKey)	String (hexString)	Dieses Datenfeld enthält den gemäß [RFC5915] in ASN.1 gemäß [X.690] DER codierte privaten Schlüssel des Datenfeldes "cert".

Tabelle 3.71 Datenfelder des Datenobjekts "Zertifikat und Schlüssel" (certAndKey)

3.22.11 Parametersatz für Schlüssel- und Zertifikats-Erzeugung

Diese Datenstruktur beschreibt die Mindestanforderungen an den Parametersatz zur Erzeugung von Schlüsselpaaren und selbstsignierten Zertifikaten.

Parameter	Datentyp	Beschreibung
Schlüsselparameter (namedCurveId) (optional)	Enumeration • BRAINPOOLP256R1 • BRAINPOOLP384R1 • BRAINPOOLP512R1 • SECP256R1 • SECP384R1	Sofern dieser optionale Parameter nicht vorhanden ist, wählt das SMGW die Standardkurve. (Standardwert: BRAINPOOLP256R1) Dieser Parameter identifiziert die für die Schlüsselpaarerzeugung und das zugehörige Zertifikat zu verwendenden kryptografischen Parameter (Bezeichnung der elliptischen Kurve). Die in der Enumeration aufgezählten Parameter sind im Rahmen der Mindestinteroperabilität zu unterstützen.
Erweiterungen (extensions) (optional)	Any	Ist dieser optionale Parameter vorhanden, kann der GWA herstellerspezifische Erweiterungen zur Erzeugung der Schlüsselpaare und des Zertifikats übergeben. Für die herstellerspezifischen Erweiterungen ist das Default-Verhalten des SMGW zu beschreiben, sofern dieser Parameter nicht vorhanden ist. Damit soll gewährleistet werden, dass das SMGW auch mit GWA-Systemen interoperabel ist, die die Erweiterungen nicht unterstützen. Siehe auch ▸ICS.FAKAT.SmgwCertMgmt.30.

Tabelle 3.72 Parameter des Profils "Schlüssel- und Zertifikatserzeugungsprofil" (cgrParameters)

Das SMGW **KANN** im Datenfeld "Erweiterungen" weitere Parameter für Schlüssel/Zertifikatserzeugungs-Parametersätze unterstützen. [REQ.FAKAT.SmgwCertMgmt.50]

Implementation Conformance Statements



ICS.FAKAT.SmgwCertMgmt.30

Der GWH **MUSS** im ICS erklären, ob das SMGW das Datenfeld Erweiterungen im Schlüssel/Zertifikatserzeugungs-Parametersatz verarbeitet. In diesem Fall muss der GWH das Verhalten des SMGW beschreiben, sofern Datenfelder mit herstellerspezifischen Erweiterungen des SMGW nicht vorhanden sind.

3.22.12 CLS-Statusliste

Diese Datenstruktur listet die im SMGW identifizierten, kommunikativ erreichbaren CLS im HAN auf.

Datenfeld	Datentyp	Beschreibung
CLS (cls)	Array [0..n] von Tupel	Enthält die Liste der CLS-Statuseinträge.
CLS-ID (clsId) (optional)	String (name)	Dieses optionale Datenfeld ist nur vorhanden, wenn eine CLS-ID konfiguriert ist oder mittels HKS.DISCOVERY ermittelt werden kann. Dieses Datenfeld identifiziert das CLS anhand eines eindeutigen Bezeichners, das als Geräteaufschrift sichtbar ist.
Linklayer-Kommunikationsadresse (l2Address) (optional)	String (hexString)	Dieses optionale Datenfeld ist nur vorhanden, wenn die Kommunikationadresse bekannt ist. Die Kommunikationsadresse ist noch nicht bekannt, wenn lediglich ein Profil hinterlegt ist aber noch keine Kommunikation stattgefunden hat. Dieses Datenfeld enthält die Kommunikationsadresse des CLS auf dem OSI Layer 2 (EUI-48 bzw. MAC-Adresse)
Netzwerklayer-Kommunikationsadresse IPv4 (ipv4Address) (optional)	String (ipv4)	Dieses optionale Datenfeld ist nur vorhanden, wenn das CLS mittels IPv4 erreichbar und die Adresse bekannt ist. Dieses Datenfeld enthält die Host-IP-Adresse des CLS im HAN.
Netzwerklayer-Kommunikationsadresse IPv6 (ipv6Address) (optional)	String (hexString)	Dieses optionale Datenfeld ist nur vorhanden, wenn das CLS mittels IPv6 erreichbar und die Adresse bekannt ist. Dieses Datenfeld enthält die IPv6-Link-Layer-Schnittstellenadresse des CLS auf dem OSI Layer 3.
ServiceList (services) (optional)	Array [1..10] von String (1..255)	Dieses optionale Datenfeld ist nur vorhanden, wenn das CLS im DNS-SD SRV-Records bereitstellt Enthält die Liste der Dienstbezeichnungen und Port-Nummern unter denen die Dienste des CLS erreichbar sind (z.B. _tlsproxy._tcp.local. 31091 [weitere Informationen])
Zusätzliche Informationen (additionalInfos) (optional)	Array [1..10] von String (1..255)	Dieses optionale Datenfeld ist nur vorhanden, wenn das CLS im DNS-SD TXT-Records bereitstellt Enthält die Liste der vom CLS im DNS-SD-TXT-Record empfangenen Attribut=Value Paare. Diese enthalten statische Geräteinformationen (z.B. Identifier)
Letzter Empfangszeitpunkt (lastTs) (optional)	String (dateTime)	Ist dieses optionale Datenfeld nicht vorhanden, wurde kein IP-Paket vom CLS empfangen. Dieses Datenfeld enthält den letzten Empfangszeitpunkt eines IP-Pakets vom CLS
Kommunikativer Anbindungsstatus (pairingState)	Enumeration • PROFILE_ONLY • IDENTIFIED • AUTHENTICATED • DATA_EXCHANGE	Dieses Datenfeld enthält Informationen über den Anbindungsstatus des CLS. Die Wertebelegungen haben folgende Bedeutung: • PROFILE_ONLY: kennzeichnet den Zustand, wenn ein Kommunikationsprofil konfiguriert ist, ohne dass das CLS im Netzwerk identifiziert wurde. • IDENTIFIED: kennzeichnet den Zustand, wenn ein CLS über eine Kommunikationsadresse erreichbar ist und noch kein Pairing über das initiale CLS-Zertifikat erfolgt ist. Da das CLS nicht authentifiziert ist, werden Listeneinträge mit diesem Anbindungsstatus nach wenigen Stunden aus der Liste entfernt. • AUTHENTICATED: kennzeichnet den Zustand, wenn das Pairing mit dem initialen CLS-Zertifikat erfolgt ist, aber vom SMGW noch keine Anwendungsnachricht verarbeitet wurde. • DATA_EXCHANGE: kennzeichnet den Zustand, wenn mindestens eine Anwendungsnachricht verarbeitet wurde.

Datenfeld	Datentyp	Beschreibung
Erweiterungen (extensions) (optional)	Any	Ist dieser optionale Parameter vorhanden, kann der GWH herstellerspezifische Erweiterungen zum Zustand der kommunikativen Anbindung des CLS ausgeben. Dieses Datenfeld enthält herstellerspezifische Statusinformationen zum Zustand der kommunikativen Anbindung des Zählers.

Tabelle 3.73 Datenfelder des Datenobjekts "CLS-Statusliste" (clsStatusList)

3.22.13 Kombiniertes Statuswort

Diese Datenstruktur beschreibt die Bedeutung von messwertbezogenen SMGW-Statusinformationen.

Datenfeld	Datentyp	Beschreibung
SMGW-Statuswort (smgwStatus)	Tupel	Das Datenfeld enthält das der Messwertverarbeitung zugeordnete 32-Bit Statuswort des SMGW gemäß E VDE-AR-N 4400:2024. Die Bits 0-31 signalisieren gemäß Statusworttyp die Informationen (Warnungen, Fehler, Status) den kombinierten Fehlerzustand aus SMGW, Messwert und Messeinrichtung.
Wert nicht validiert (valueNotValidated)	Boolean	Wenn dieser Status "true" ist dürfen die Messwerte nicht zu Abrechnung verwendet werden. Entspricht Bit 1. Standardwert: false.
Fataler Fehler SMGW (error)	Boolean	Wenn dieser Status "true" ist, hat das SMGW im Selbsttest einen fatalen Fehler erkannt, sodass die im Rahmen der Konformitätsbewertung überprüfte Messfunktionalität jetzt und in Zukunft nicht mehr gewährleistet ist (z.B. erkannter Fehler bei Hashwertprüfung der Firmware). Eine Wiederherstellung der konformitätsbewerteten Messfunktionalität ist nicht selbsttätig durch das SMGW oder durch einen Neustart möglich. Entspricht Bit 8. Standardwert: false.
SMGW Systemzeit ungültig (timeNotValid)	Boolean	Wenn dieser Status "true" ist, erfüllt die Systemzeit des SMGW zum Zeitpunkt der Zeitstempelung nicht die Vorgaben zur Verwendung im geschäftlichen Verkehr. Entspricht Bit 9. Standardwert: false.
Warnung SMGW (warning)	Boolean	Wenn dieser Status "true" ist, hatte das SMGW zum Zeitpunkt der Messwertregistrierung keine gültige Systemzeit. Entspricht Bit 12. Standardwert: false.
Fehlender Wert (noValue)	Boolean	Wenn dieser Status "true" ist, wurde vom SMGW innerhalb des Akzeptanzzeitfensters kein Messwert registriert. Entspricht Bit 13. Standardwert: false.
Manipulationserkennung SMGW (tamper)	Boolean	Wenn dieser Status "true" ist, wurde der Messwert durch magnetische oder mechanische Manipulation gestört (z.B. Klemmdeckel geöffnet). Entspricht Bit 14. Standardwert: false.
Schwellwertauslösung (valueTriggered)	Boolean	Wenn dieser Status "true" ist, wurde der Messwert aufgrund einer Schwellwertverletzung versandt. Entspricht Bit 16. Standardwert: false.
Zählerstatuswort (meterStatusWord)	String (hexString)	Das Datenfeld enthält das 32 Bit Statuswort der Messeinrichtung gemäß E VDE-AR-N 4400:2024. Bit 0-7 definieren die Typ der Messeinrichtung und die darüber differenzierte Bedeutung der Bits 8-31. Bit 0 hat die niedrigste Wertigkeit, Bit 31 die höchste Wertigkeit.

Tabelle 3.74 Datenfelder des Datenobjekts "Kombiniertes Statuswort aus SMGW- und Zählerstatuswort" (combinedStatus)

3.22.14 Parametersatz für CSR-Erzeugung

Diese Datenstruktur beschreibt die Mindestanforderungen an den Parametersatz zur Erzeugung von Schlüsselpaaren und Certificate Signing Requests (CSR) für PKI-Zertifikate.

Parameter	Datentyp	Beschreibung
Schlüsselparameter (namedCurveId) (optional)	Enumeration • BRAINPOOLP256R1 • BRAINPOOLP384R1 • BRAINPOOLP512R1	Sofern dieses optionale Datenfeld nicht vorhanden ist, wählt das SMGW gemäß [TR-03109-3] die kürzeste zulässige Schlüssellänge für SM-PKI Zertifikate. (Standardwert: BRAINPOOLP256R1) Dieses Datenfeld identifiziert die für die Schlüsselpaarerzeugung für den CSR zu verwendenden kryptografischen Parameter (Bezeichnung der elliptischen Kurve). Die in der Enumeration aufgezählten Parameter sind im Rahmen der Mindestinteroperabilität zu unterstützen.
Issuer Zertifikat (issuerCert)	String (hexString)	X.509 (Signatur-)Zertifikat der Sub-CA (SUBCA_SIG_CRT) an die der CSR gesendet wird, dessen AuthorityKeyIdentifier in den zu erzeugenden CSR übernommen wird.
Organisationseinheit (ou) (optional)	String (1..64)	Sofern dieser optionale Parameter nicht vorhanden ist, verwendet das SMGW den Inhalt des Subject Distinguished Name Attributes CN (CommonName) aus dem aktuellen im SMGW gespeicherten GWA-Zertifikat (GWA_WAN_TLS_CRT). Dieses Datenfeld wird in das Attribut "OU" des zu erzeugenden CSR übernommen und identifiziert den für das SMGW verantwortlichen Administrator (siehe [SM-PKI-CP] Anhang A).
Erweiterungen (extensions) (optional)	Any	Ist dieser optionale Parameter vorhanden, kann der GWA herstellerspezifische Erweiterungen zur Erzeugung der Schlüsselpaare und des CSR übergeben. Für die herstellerspezifischen Erweiterungen ist das Default-Verhalten des SMGW zu beschreiben, sofern dieser Parameter nicht vorhanden ist. Damit soll gewährleistet werden, dass das SMGW auch mit GWA-Systemen interoperabel ist, die die Erweiterungen nicht unterstützen. Siehe auch ▸ICS.FAKAT.SmgwCertMgmt.20.

Tabelle 3.75 Parameter des Profils "CSR-Erzeugungsprofil" (csrParameters)

Das SMGW **KANN** im Datenfeld "Erweiterungen" weitere Parameter für CSR-Parametersätze unterstützen. [REQ.FAKAT.SmgwCertMgmt.20]

Implementation Conformance Statements



ICS.FAKAT.SmgwCertMgmt.20

Der GWH **MUSS** im ICS erklären, ob das SMGW das Datenfeld Erweiterungen im CSR-Parametersatz verarbeitet. In diesem Fall muss der GWH das Verhalten des SMGW beschreiben, sofern Datenfelder mit herstellerspezifischen Erweiterungen des SMGW nicht vorhanden sind.

3.22.15 Device-Info

Die Datenstruktur "Device-Info" dient der Ausgabe von Informationen über das SMGW oder angeschlossene Geräte, die beispielsweise im Rahmen von Konformitätsbewertungsverfahren referenziert werden können.

Datenfeld	Datentyp	Beschreibung
Profil-ID (profileId)	String (name)	Dieses Datenfeld identifiziert das DeviceInfo-Profil unter allen DeviceInfo-Profilen an den Schnittstellen des SMGW eindeutig. Sofern nur ein DeviceInfo Profil im SMGW vorhanden ist, entspricht die Profile-ID der SMGW-ID. Dieses Datenfeld wird als Ressourcen-Identifikation verwendet.
Geräte-ID (deviceId)	String (huid)	Dieser Parameter identifiziert das Gerät, das der Geräte-Information zugeordnet ist.

Datenfeld	Datentyp	Beschreibung
Hersteller (mfct)	String (3..3)	Dieses Datenfeld enthält die Kurzbezeichnung des Herstellers des Gerätes
Produktions-Charge (batch) (optional)	String (1..32)	Sofern die Charge nicht bestimmt werden kann, ist dieses Datenfeld nicht vorhanden. Dieses Datenfeld enthält die Bezeichnung der Produktions-Charge des Gerätes
Softwareversion (sw-Versions)	Array [0..n] von Tupel	Dieses Datenfeld enthält die Liste der auf dem Gerät vorhandenen Software-Versionen inkl. ihres Aktivierungs-Zustandes
Identifikation der Firmware (fwId)	String (1..32)	Version oder Identifikation der Firmware
Firmware ist aktiv (active) (optional)	Boolean	Fehlt dieses Datenfeld, ist die Software aktiv (Standardwert: true) Ist dieses Datenfeld "true", so ist die Software aktiv
Komponenten (components)	Array [0..n] von Tupel	Dieses Datenfeld enthält die Typbezeichnung, Hersteller, SW-Version, HW-Version, Seriennummer der SMGW-Komponenten. Datenfeld kann dafür verwendet werden, zu entscheiden, ob eine bestimmte per Update einzuspielende Softwareversion kompatibel zur vorliegenden Hardware ist.
Typ der Komponente (componentType)	String (1..32)	Dieses Datenfeld enthält den Namen/Typ der Hardware-Komponente
Hersteller (mfct)	String (1..32)	Dieses Datenfeld enthält den Namen des Herstellers
SW-Version (swVersion) (optional)	String (1..32)	Sofern keine Software-Version bestimmt werden kann, ist dieses optionale Datenfeld leer. Dieses Datenfeld enthält die SW-Versionsnummer der Komponente
HW-Version (hwVersion) (optional)	String (1..32)	Sofern keine Hardware-Version bestimmt werden kann, ist dieses optionale Datenfeld leer. Dieses Datenfeld enthält die HW-Versionsnummer der Komponente
Seriennummer (serialNo) (optional)	String (1..32)	Sofern keine Seriennummer bestimmt werden kann, ist dieses optionale Datenfeld leer. Dieses Datenfeld enthält die Seriennummer der Komponente
Max. Firmware-Größe (maxFwSize) (optional)	Integer (0..2147483647)	Ist dieses Datenfeld nicht vorhanden, wird der Maximalwert (unbegrenzt) angenommen Dieses Datenfeld enthält eine Angabe in Bytes, die angibt, welche Firmware-Dateigröße im Gerät installiert werden kann. Ein Wert 0 bedeutet, dass keine Firmware installiert werden kann.
Erweiterungen (extensions) (optional)	Any	Ist dieses Datenfeld vorhanden, können herstellerspezifische Erweiterungen verwendet werden. Das Datenfeld dient der Ausgabe weiterer Informationen. Siehe auch ▸ICS.FAKAT.SmgwMonitoring.10.

Tabelle 3.76 Datenfelder des Datenobjekts "DeviceInfo" (deviceInfo)

Implementation Conformance Statements



ICS.FAKAT.SmgwMonitoring.10

Der GWH **MUSS** im ICS erklären, ob das SMGW im Datenfeld "Erweiterungen" der SMGW-Informationen weitere Informationen bereitstellt. In diesem Fall muss der GWH die Bedeutung der Informationen beschreiben.

3.22.16 Device-Status

Die Datenstruktur "Device-Status" dient der Ausgabe des aktuellen Gerätestatuswortes des SMGW oder einer Messeinrichtung. Die Informationen können beispielsweise im Rahmen von Konformitätsbewertungsverfahren referenziert werden können.

Datenfeld	Datentyp	Beschreibung
Geräte-ID (deviceId)	String (huid)	Dieses Datenfeld enthält die Identifikation des Gerätes gemäß DIN43849
Statuswort (statusWord)	String (hexString)	Dieses Datenfeld enthält das Gerätestatuswort gemäß TR-03109-1-DS Kapitel Messwertstatus Bit 0 ist das niederwertigste Bit

Tabelle 3.77 Datenfelder des Datenobjekts "DeviceStatus" (deviceStatus)

3.22.17 Exportstruktur

Sofern Messwerte zur Zwischenspeicherung außerhalb des SMGW oder zur Nichtabstreitbarkeit der Herkunft und Vollständigkeit signiert werden, werden diese in einer signierten Datenstruktur an den Empfänger übermittelt.

Dies folgende Datenstruktur dient als Container beim Export der gesamten oder einer Teilmenge von Messwerten einer Werteliste.

Datenfeld	Datentyp	Beschreibung
SMGW-ID (gatewayId) (optional)	String (huid)	Dieses Datenfeld ist beim Export im HAN vorhanden und entfällt beim Export ins WAN. Dieses Datenfeld enthält die herstellerübergreifende Identifikation des SMGW, das diese Datenstruktur erstellt hat.
Anwendungsreferenz (tafId) (optional)	Tupel	Dieser Parameter entfällt beim Export von Logbüchern und ist beim Export von Messwertlisten RWL, NWL, AWL vorhanden. Der Inhalt dieses Parameters wird beim Versand der Messwerte an den EMT übermittelt, damit der berechtigte Empfänger einen Bezug zwischen bestellter Konfiguration und zugelieferten Werten herstellen kann. Die Zuordnung der Identifikation zu Anschlussnutzern findet beim berechtigten Empfänger statt.
Identifikation des Marktpartners (mpId)	String (name)	Dieser Parameter enthält eine Identifikation des Marktpartners (Für den Strommarkt: Siehe bdew-codes.de). Der Marktpartner ist zu unterscheiden vom Empfänger der Messwerte (siehe "Zugeordnetes WAN-Kommunikationsprofil"), da dieser die Messwerte ggf. über einen Dritten erhält. Er dient dem Anschlussnutzer als Transparenzinformation für versandte Werte.
Zählpunktbezeichnung (meteringPointId)	String (name)	Dieses Datenfeld enthält den eindeutigen Bezeichner der Messlokation gemäß [VDE44400].
Marktpartner-Rolle (mpRole)	String (name)	Dieses Datenfeld enthält die Rolle des Marktpartners gemäß [VDE44400].
MSB spezifisch (msbSpecific) (optional)	String (name)	Ist dieses Optionale Datenfeld nicht vorhanden, wird die Anwendungsreferenz mit "0" aufgefüllt. Dieses Datenfeld enthält die vom MSB vergebene Referenz zur Zuordnung der Versandten Messwerte.
Exportdaten (exportedData)	Tupel	Dieses Datenfeld enthält die zu exportierenden Daten. Der Datentyp wird explizit über dieses Datenfeld bestimmt. Es sind nur die folgenden Datentypen/Datenstrukturen zulässig.

Datenfeld	Datentyp	Beschreibung
Hierunter werden die zu exportierenden Daten in der Datenstruktur einsortiert. Es ist zu beachten, dass zwar auf andere Datenstrukturen verwiesen wird, jedoch nicht zwingend alle Einträge der Datenstruktur Teil des Exports werden. Dies ist vom exportierten Zeitraum abhängig. Folgende Elemente sind an dieser Stelle möglich: • RegisteredReadingList (definiert in ▸Tabelle 3.100) • NonValidatedReadingList (definiert in ▸Tabelle 3.96) • Logbook (definiert in ▸Tabelle 3.87) • DailyMeterReadingList (definiert in ▸Tabelle 3.108) • DerivedValueList (definiert in ▸Tabelle 3.65)		
Signatur (signature) (optional)	Tupel	Dieses optionale Datenfeld ist vorhanden, wenn die exportierte Nachricht signiert ist. Für die Aufbewahrung oder Weiterleitung von Inhaltsdaten gewährleistet die Signatur die Authentifizität und Herkunft der Nachricht. Dieses Datenfeld enthält die Informationen, die zur Signaturprüfung benötigt werden.
Verfahren (algo)	Enumeration • CMS_ECDSA_SHA256_Detached	Bezeichnet das Verfahren mit dem die Berechnung und Codierung der Signatur durchgeführt werden (Siehe Detailspezifikation CMS).
Zeitstempel der Signatur (ts)	String (dateTime)	Dieses Datenfeld enthält den Zeitpunkt, zu dem die Signatur erstellt wurde.
Signaturersteller (originator)	String (huid)	Identifiziert den Ersteller der Signatur und ist mit der kryptografischen Identität des Signaturschlüssels verknüpft, mit der die Signatur erstellt wurde. Das Signaturzertifikat mit dem öffentlichen Schlüssel ist Teil der CMS-Datenstruktur "SignedData".
Signaturwert (sigValue)	String (hexString)	Die Signatur wird über den Hash des kanonisierten Tupels über alle oben genannten Datenfelder gebildet. Die Anzuwendende Kanonisierung von JSON ist in der Detailspezifikation Webservice beschrieben. Bei der Kanonisierung wird durch Weglassen von Whitespace außerhalb von Strings eine Normalisierung vor der Hash-Berechnung hergestellt. Die Bildung und Codierung der Signatur ergibt sich aus dem Datenfeld "Verfahren". Für CMS_ECDSA_SHA256_Detached enthält dieses Datenfeld codiert das Signaturzertifikat des Signaturerstellers, den Signatur- und Hashalgorithmus, den Hash über die kanonisierten oben genannten Datenfelder und den Signaturwert.

Tabelle 3.78 Datenfelder des Datenobjekts "Exportstruktur" (exportStructure)

3.22.18 Firmware-Update-Profil

Ein Firmware-Update-Profil beschreibt die Konfigurationsparameter, die das Verhalten des SMGW zum Download und zur Aktualisierung der Firmware (und der damit verbundenen statischen Konfiguration) beeinflussen.

Parameter	Datentyp	Beschreibung
Profil-ID (profileId)	String (name)	Dieses Datenfeld identifiziert das Firmware-Update Profil unter allen Firmware-Update Profilen an den Schnittstellen des SMGW eindeutig. Dieses Datenfeld dient als Ressourcen-Identifikation.
Geräte-ID (deviceId)	String (huid)	Identifiziert die Komponente, für die das Firmware-Update bestimmt ist.
Download-Adresse (downloadUri)	String (absolute-uri)	https-URI (IP-Adresse, Portnummer, Pfad) unter der das SMGW eine (Firmware-)Datei vom Fileserver abrufen kann.

Parameter	Datentyp	Beschreibung
Download Startzeitpunkt (downloadTime) (optional)	String (dateTime)	Sofern dieses optionale Datenfeld nicht angegeben ist, wird der Download unmittelbar nach Import des Firmwaredownload-Profiles gestartet. Zeitpunkt nach dem der Download von der Download-Adresse beginnt.
Installation Startzeitpunkt (timeOfActivation) (optional)	String (dateTime)	Sofern dieses optionale Datenfeld nicht angegeben ist, wird der Update unmittelbar nach vollständigem Download gestartet. Zeitpunkt, nach dem der Update beginnt, sofern der vorangegangene Download vollständig ist.
Erweiterungen (extensions) (optional)	Any	Ist dieser optionale Parameter vorhanden, kann der GWA herstellerspezifische Erweiterungen zur Steuerung des Firmware-Updates übergeben. Herstellerspezifische Erweiterungen

Tabelle 3.79 Parameter des Profils "Firmware-Update Profil" (firmwareUpdateProfile)

Das SMGW **KANN** im Datenfeld "Erweiterungen" weitere Parameter für das Firmware-Update-Profil unterstützen (▸ICS.FAKAT.FwDownload.10). [REQ.FAKAT.FwDownload.20]

Implementation Conformance Statements



ICS.FAKAT.FwDownload.10

Der GWH **MUSS** im ICS erklären, ob das SMGW das Datenfeld Erweiterungen im Firmware-Update-Profil verarbeitet. In diesem Fall muss der GWH das Verhalten des SMGW beschreiben, sofern Datenfelder mit herstellerspezifischen Erweiterungen des SMGW nicht vorhanden sind.

3.22.19 GWA-Wechselparameter

Datenstruktur für die Übermittlung der Parameter zum GWA-Wechsel.

Parameter	Datentyp	Beschreibung
Wechselzeitpunkt (switchTime) (optional)	String (dateTime)	Sofern dieses optionale Datenfeld nicht vorhanden ist, wird der Wechsel sofort ausgelöst. Dieses Datenfeld gibt den Zeitpunkt an, zu dem der Wechsel vom SMGW ausgelöst werden soll
Maximale Bestätigungsdauer (switchTimeout) (optional)	Integer (60..2678400)	Sofern dieses optionale Datenfeld nicht vorhanden ist, wird der Standardwert angenommen. (Standardwert: 86400) Dieses Datenfeld gibt die maximale Zeitdauer (in Sekunden) an, bis zu der eine erfolgreiche Bestätigung der Akzeptanz des Wechselprozesses durch den künftigen GWA erfolgt sein muss. Erfolgt innerhalb dieses Zeitraumes keine Bestätigung wird der Wechsel nicht durchgeführt.

Tabelle 3.80 Parameter des Profils "GWA-Wechselparameter" (gwaSwitchParameters)

3.22.20 GWA-Zertifikatssatz

▸Tabelle 3.81 beschreibt die Bedeutung des Inhaltes eines Zertifikatssatzes der SM-PKI für einen GWA.

Parameter	Datentyp	Beschreibung
CV-Zertifikat zum Import des TLS-Zertifikatsschlüssels (tlsKeyCvCert)	String (hexString)	Enthält eine CV-Datenstruktur (siehe [TR-03109-2]) zum Import des TLS-Public-Keys in das Sicherheitsmodul des SMGW.
CV-Zertifikat zum Import des Signaturzertifikatsschlüssels (sigKeyCvCert)	String (hexString)	Enthält eine CV-Datenstruktur (siehe [TR-03109-2]) zum Import des SIG-Public-Keys in das Sicherheitsmodul des SMGW.

Parameter	Datentyp	Beschreibung
CV-Zertifikat zum Import des Verschlüsselungszertifikatsschlüssels (encKeyCvCert)	String (hexString)	Enthält eine CV-Datenstruktur (siehe [TR-03109-2]) zum Import des ENC-Public-Keys in das Sicherheitsmodul des SMGW.
CV-Zertifikat zum Import des Authentifizierungszertifikatsschlüssels (autKeyCvCert)	String (hexString)	Enthält eine CV-Datenstruktur (siehe [TR-03109-2]) zum Import des AUT-Public-Keys in das Sicherheitsmodul des SMGW. (Der Schlüssel entspricht dem TLS-Public-Key, das CV-Zertifikat unterscheidet sich aufgrund der KeyReference).

Tabelle 3.81 Parameter des Profils "GWA-Zertifikatssatz" (gwaCertificateSet)

3.22.21 HAN-Schnittstellenkonfigurationsprofil

HAN-Schnittstellenkonfigurationsprofile legen die Parameter für die Konfiguration der HAN-Schnittstelle des SMGW fest.

Parameter	Datentyp	Beschreibung
Profil-ID (profileId)	String (name)	Der im SMGW eindeutige Bezeichner des HAN-Schnittstellenkonfigurationsprofils.
Schnittstellenbezeichnung (ifName)	String (name)	Im SMGW eindeutige Bezeichnung der physischen HAN-Schnittstelle. Beginnt mit "HAN". "HAN-CON" ist die für den Endnutzer zugängliche Schnittstelle, "HAN-CLS" die für den Endkunden nicht zugängliche Schnittstelle.
Host-IPv4-Adresskonfiguration (hostIpv4Addr) (optional)	Tupel	Fehlt dieser optionale Parameter, werden die Standardwerte der Unterparameter verwendet. Legt fest, wie das SMGW die IPv4-Adresse der HAN-Schnittstelle bestimmt.
Modus (mode) (optional)	Enumeration • AutoIP • Static • DHCP	Ist der Parameter leer, wird AutoIP angenommen. (Standardwert: AutoIP) Legt die Betriebsart fest, wie das SMGW die IP-Adresse(n) der HAN-Schnittstelle bestimmt. Die Wertebelegungen haben folgende Bedeutung: • AutoIP: Wird "AutoIP" angegeben, wird für IPv4 das Verfahren nach RFC3927 verwendet. • Static: Wird "Static" angegeben, wird die im Datenfeld ip4Addr angegebene Adresse statisch verwendet. • DHCP: Wird "DHCP" angegeben, versucht das SMGW für die HAN-Schnittstelle als DHCPv4-Client eine IPv4-Adresse und für IPv4 eine Subnetzmaske von einem DHCP-Server zu erhalten.
IPv4-Adresse (ip4Addr) (optional)	String (ipv4)	Dieser Parameter wird für den Adressmode "Static" benötigt. Legt die IPv4-Adresse der Schnittstelle als Dotted-Decimal-Notation fest.
IPv4-Subnetzmaske (ip4Mask) (optional)	String (ipv4)	Dieser Parameter wird für den Adressmode "Static" benötigt. Wird er nicht angegeben wird eine Punkt-zu-Punkt Subnetzmaske verwendet. (Standardwert: 255.255.255.255) Legt die IPv4-Subnetzmaske der Schnittstelle als Dotted-Decimal-Notation fest.
Maximale Authentifizierungsversuche (authAttempts) (optional)	Integer (1..10)	Sofern dieses optionale Datenfeld nicht vorhanden ist, wird der vom Hersteller im ICS angegebene Wert verwendet. Maximale Zahl der fehlerhaften Authentifizierungsversuche mittels Username/Password, bevor das SMGW weitere Authentifizierungsversuche für die konfigurierte Wartezeit ablehnt. Siehe auch ▸ICS.HAN.SicherungKommunikationConSrv.50.

Parameter	Datentyp	Beschreibung
Wartezeit nach Authentifizierungsfehlern (authFailWait) (optional)	Integer (0..600)	Sofern dieses optionale Datenfeld nicht vorhanden ist, wird der vom Hersteller im ICS angegebene Wert verwendet. Dauer (in Sekunden) bei Erreichen der max. fehlerhaften Authentifizierungsversuche, bevor wieder neue Authentifizierungen durchgeführt werden können. Wird ein Wert 0 angegeben, sind weitere Authentifizierungsversuche ohne Wartezeit möglich. Siehe auch ▸ICS.HAN.SicherungKommunikationConSrv.60.
TCP-Ports für Dienste des SMGW im HAN		
Port für HKS.TLSPROXY.SOCKS (socksPort) (optional)	Integer (1..65534)	Sofern dieses optionale Datenfeld nicht vorhanden ist, wird der Well-Known Port 1080 verwendet. Der Port, auf dem das SMGW im HAN den TLS-SOCKS-Dienst anbietet
Port für HKS.NTP-TLS.SRV (ntpTlsPort) (optional)	Integer (1..65534)	Sofern dieses optionale Datenfeld nicht vorhanden ist, wird der Well-Known Port 4460 (NTS-KE) verwendet. Der Port, auf dem das SMGW im HAN den Zeitservice NTP-TLS anbietet
Port für HKS.TLSPROXY.SRV (tlsProxyPort) (optional)	Integer (1..65534)	Sofern dieses optionale Datenfeld nicht vorhanden ist, wird der Port 31091 verwendet. Der Port, auf dem das SMGW an der Schnittstelle den TLS-Proxy-Dienst anbietet
Port für HKS.WS1 und HKS.WS2 (httpsPort) (optional)	Integer (1..65534)	Sofern dieses optionale Datenfeld nicht vorhanden ist, wird der Well-Known Port 443 verwendet. Der Port, auf dem das SMGW an der Schnittstelle http-Webservices anbietet
Erweiterungen (extensions) (optional)	Any	Ist dieser optionale Parameter vorhanden, kann der GWA herstellerspezifische Erweiterungen zur Verbindungsherstellung übergeben, die im SMGW persistiert werden. Für die herstellerspezifischen Erweiterungen ist das Default-Verhalten des SMGW zu beschreiben, sofern dieser Parameter nicht vorhanden ist. Damit soll gewährleistet werden, dass das SMGW auch mit GWA-Systemen interoperabel ist, die die Erweiterungen nicht unterstützen.

Tabelle 3.82 Parameter des Profils "HAN-Schnittstellenkonfigurationsprofil" (hanIfProfile)

Das SMGW kann im Datenfeld "Erweiterungen" weitere Parameter für Schnittstellenkonfigurationsprofile unterstützen.

ICS



ICS.HAN.IfProfile.10

Der GWH **MUSS** im ICS erklären, ob das SMGW das Datenfeld Erweiterungen im HAN-Schnittstellenkonfigurationsprofil verarbeitet. In diesem Fall muss der GWH das Verhalten des SMGW beschreiben, sofern Datenfelder mit herstellerspezifischen Erweiterungen des SMGW nicht vorhanden sind.



ICS.HAN.SicherungKommunikationConSrv.50

Der GWH **MUSS** im ICS deklarieren, nach welcher Zahl erfolgloser Zugriffsversuche das SMGW gemäß ▸authAttempts (Default) vorübergehend keine Zugriffsversuche mehr akzeptiert.



ICS.HAN.SicherungKommunikationConSrv.60

Der GWH **MUSS** im ICS deklarieren, für welchen Zeitraum das SMGW gemäß ▸authFailWait (Default) keine weiteren Zugriffsversuche akzeptiert (In Sekunden).

3.22.22 HAN-Kommunikationsprofil

HAN-Kommunikationsprofile legen die Parameter für die Kommunikation von Anschlussnutzern und Servicetechnikern mit dem SMGW im HAN fest.

Parameter	Datentyp	Beschreibung
Profil-ID (profileId)	String (name)	Dieses Datenfeld identifiziert das HAN-Kommunikationsprofil unter allen HAN-Kommunikationsprofilen an den Schnittstellen des SMGW eindeutig. Dieses Datenfeld wird als Ressourcen-Identifikation verwendet.
Rolle (role)	Enumeration • CON • SRV • CLS	Legt die Rolle des lokalen Nutzers beim Zugriff auf die Dienste des SMGW fest. Die Wertebelegungen haben folgende Bedeutung: • CON: bezeichnet die Rolle "Endkunde" (Letztverbraucher: Anschlussnutzer/Anlagenbetreiber) • SRV: bezeichnet die Rolle Servicetechniker des SMGW. • CLS: bezeichnet die Rolle eines lokalen steuerbaren Systems.
Kommunikationsszenario (ks)	Enumeration • WS1 • WS2 • NTP-TLS • TLSPROXY.SOCKS • TLSPROXY.SRV • TLSPROXY.CLI	Legt das Kommunikationsszenario fest. Die zulässige Wertebelegung ist von der verwendeten Rolle abhängig und wird beim Einspielen des Profils überprüft. Siehe auch ▸Abschnitt 4.4.2. Die Wertebelegungen haben folgende Bedeutung: • WS1: TLS-gesicherter HTTP-Server mit Client-Zertifikatsauthentifizierung (entspricht dem bisherigen HKS1). • WS2: TLS-gesicherter HTTP-Server mit Digest-Authentifizierung (entspricht dem bisherigen HKS2). • NTP-TLS: Durch das SMGW bereitgestellter NTP-Server. • TLSPROXY.SOCKS: Proxy-Kanal mit Verbindungsaufbau durch das CLS unter Verwendung von SOCKS (entspricht dem bisherigen HKS3). • TLSPROXY.SRV: Proxy-Kanal mit Verbindungsaufbau durch das CLS unter Verwendung von TLS-SNI. • TLSPROXY.CLI: Proxy-Kanal Verbindungsaufbau durch das SMGW (entspricht dem bisherigen HKS4 und HKS5).
Kennung des lokalen Nutzers (userId) (optional)	String (name)	Dieser Parameter ist für die Rollen "CON" und "CLS" verpflichtend anzugeben, für andere Rollen (SRV) entfällt er. Für die Rolle CON identifiziert dieser Parameter die eindeutige Kennung des lokalen Nutzers (Anschlussnutzer, Endkunde), die zur Verknüpfung mit dem Auswertungsprofil und UserLog verwendet wird. Für die Rolle CLS identifiziert dieser Parameter die eindeutige Gerätekennung des CLS (CLS-ID).
Authentifizierungsparameter für Kommunikationsszenarien WS1, TLSPROXY.SOCKS, TLSPROXY.SRV und TLSPROXY.CLI		

Parameter	Datentyp	Beschreibung
Zertifikat(e) zur TLS-Authentifizierung des Kommunikationspartners (peerCert) (optional)	Array [1..2] von String (hexString)	Dieser optionale Parameter ist nur für die Kommunikationsszenarien WS1, TLSPROXY.SOCKS, TLSPROXY.SRV und TLSPROXY.CLI vorhanden. Dieser Parameter enthält das Zertifikat zur Verifikation der Authentizität des Kommunikationspartners. Dies kann ein Endnutzerzertifikat oder ein CA-Zertifikat sein. Endnutzerzertifikat: Zertifikat für die TLS-Authentifizierung des Kommunikationspartners durch das SMGW (Direct-Trust). CA-Zertifikat: Das Signatur-Zertifikat einer CA, mit dem ein kurzlebiges Zertifikat des Servicetechnikers validiert werden kann. Im Überlappungszeitraum des Zertifikatswechsels kann sich der Kommunikationspartner mit einem der Zertifikate authentifizieren. Die Anforderungen an HAN-Zertifikatsprofile sind in der Detailspezifikation (Zertifikatsprofile im HAN) beschrieben.
Authentifizierungsparameter für Kommunikationsszenario WS2		
Nutzerauthentifizierung (userCredentials) (optional)	Array [1..2] von Tupel	Dieser optionale Parameter ist nur für das Kommunikationsszenario WS2 vorhanden. Enthält die zur Überprüfung der Identität und Authentizität des anfragenden Nutzers notwendigen Informationen, wie z.B. Information über das Authentifizierungsschema, Passwort-Hash, User-/Accountname und Passwort. Für das HTTP Digest-Authentifizierungsverfahren ist es nicht erforderlich, dass das SMGW Kenntnis des Passwortes selbst hat.
Authentifizierungsschema (authScheme)	Enumeration • HTTP_DIGEST_MD5 • HTTP_DIGEST_SHA256	Authentifizierungsschema gemäß Detailspezifikation. Das Authentifizierungsschema legt die Bedeutung der folgenden Parameter fest. Die Wertebelegungen haben folgende Bedeutung: • HTTP_DIGEST_MD5: Digest-Authentification mit MD5 (deprecated) • HTTP_DIGEST_SHA256: Digest-Authentication mit SHA256
Username (username) (optional)	String (name)	Sofern dieser optionale Parameter nicht vorhanden ist, wird für ein CON-Kommunikationsprofil die Kennung des lokalen Nutzers (userId) verwendet. Dieser Parameter enthält den Namen, der für die Identifizierung und Authentifizierung des lokalen Nutzers verwendet wird.
Hash (hash) (optional)	String (hexString)	Beim Einspielen eines neuen Profils ist dieser Parameter verpflichtend anzugeben. Beim Aktualisieren eines bestehenden Profils kann dieser Parameter ausgelassen werden, sodass der Wert unverändert bleibt. Beim Auslesen des Profils ist der Parameter nie vorhanden. Bei http-Digest-Authentifizierung enthält dieser Parameter den Hash HA1 = Hash(<userName>:<realm>:<password>). <realm> entspricht der kanonisierten SMGW-ID (lowercase)
Kommunikationsparameter für alle Kommunikationsszenarien		
Verbindung halten (keepOpen) (optional)	Boolean	Wird dieser optionale Parameter nicht angegeben, dann wird der Standardwert verwendet. (Standardwert: true) Legt fest, ob die TLS-Verbindung dauerhaft aufrechterhalten werden soll (true), auch wenn die Aktion, die zum Aufbau geführt hat, nicht mehr gegenwärtig ist. Die TLS-Verbindung wird erst dann geschlossen, wenn die maximale Sitzungsdauer erreicht ist. Siehe auch ▸ICS.WAN.Kommunikationsprofil.20.

Parameter	Datentyp	Beschreibung
Wartezeit im Leerlauf (idleTimeout) (optional)	Integer (0..999999)	Wird dieser optionale Parameter nicht angegeben, dann werden Verbindungen, bei denen das SMGW TLS-Server ist, nach der Standardzeit im Leerlauf abgebaut. (Standardwert: 300) Nach Ablauf der Zeit (in Sekunden) im Leerlauf, wird die TLS-Verbindung wieder abgebaut. Der Wert 0 deaktiviert den Abbau im Leerlauf.
Maximale Sitzungsdauer (maxSessionDuration) (optional)	Integer (0..172800)	Wird dieser optionale Parameter nicht angegeben, dann wird der Standardwert angenommen. (Standardwert: 0) Die maximale Zeit (in Sekunden), die eine TLS-Sitzung aufrechterhalten werden soll, bzw. nach der ein lokaler Authentifizierter Nutzer ausgeloggt wird. Der Wert 0 beschränkt die Sitzungszeit auf die für die gewählten TLS-Protokollparameter zulässige Dauer. Das Verhalten des SMGW bei Kombinationen von keepOpen, idleTimeout und maxSessionDuration ist in den Anforderungen bei HAN-Verbindungen beschrieben. Siehe auch ▸REQ.HAN.Transport.80.
Kommunikationsparameter für abgehende Verbindungen (nur vorhanden bei HKS.TLSPROXY.CLI)		
Kommunikationsparameter für abgehende Verbindungen im HAN (outboundConnection) (optional)	Tupel	Dieser optionale Parameter ist nur für HKS.TLSPROXY.CLI vorhanden Beschreibt die Kommunikationsparameter für abgehende HAN-Verbindungen
Adresse des Kommunikationspartners CLS (address)	String (absolute-uri)	Dieser Parameter legt eine Adresse (Portnummer, IPv4-, IPv6-Adresse oder einen DNS-Hostnamen) fest zu der eine TLS-Verbindung vom SMGW aufgebaut werden muss. Unter dieser Adresse bietet ein CLS Dienste für das SMGW an. Der Hostname wird für die mDNS/DNS-SD-Adresssauflösung verwendet. Für TLS-Proxy Dienste wird das URI-Schema "tlsproxy" verwendet.
Wiederholung fehlgeschlagener Verbindungsversuche (retryConfig) (optional)	Tupel	Ist dieser optionale Parameter nicht angegeben, gelten die Defaults der folgenden Datenfelder Bestimmt die Anzahl und Dauer zwischen den Versuchen zum Aufbau einer Transportverbindung.
Anzahl Runden (maxLoopCount) (optional)	Integer (1..65535)	Fehlt dieser optionale Parameter, wird eine Wiederholungsrunde durchgeführt (Standardwert: 1) Maximale Anzahl der Runden der Retries. Die maximale Gesamtzahl der Versuche ist maxLoopCount * maxRetryCount.
Protokollierung wenn die zweite oder eine weitere Runde gestartet wird (logLoopFailures) (optional)	Boolean	Fehlt dieser optionale Parameter, wird der Standardwert verwendet. (Standardwert: true) Ist der Wert "true", erfolgt ein Eintrag ins Logbuch, wenn die zweite oder eine weitere Runde gestartet wird.
Wartezeit zwischen zwei Runden (loopDelay) (optional)	Array [1..16] von Integer (0..86400)	Fehlt dieser optionale Parameter, wird der Standardwert verwendet. (Standardwert: 3600) Legt die Wartezeit zwischen zwei Runden fest (in Sekunden). Der erste Listeneintrag bestimmt die Wartezeit zwischen Runde 1 und Runde 2. Der zweite zwischen Runde 2 und Runde 3, usw. Die maximale Anzahl von Einträgen wird vom GWH im ICS beschrieben. Sind weniger Einträge als maxLoopCount vorhanden, wird der letzte Eintrag für die weiteren Runden verwendet.

Parameter	Datentyp	Beschreibung
Maximale Anzahl Wiederholversuche innerhalb einer Runde (maxRetryCount) (optional)	Integer (1..65535)	Fehlt dieser optionale Parameter wird der Standardwert verwendet. (Standardwert: 10) Maximale Anzahl der Retries innerhalb einer Runde.
Protokollierung wenn die zweite oder eine weitere Wiederholung gestartet wird (logRetryFailures) (optional)	Boolean	Fehlt dieser optionale Parameter, wird der Standardwert verwendet. (Standardwert: true) Ist der Wert "true", erfolgt ein Eintrag ins Logbuch, wenn die zweite oder eine weitere Wiederholung in einer Runde gestartet wird.
Wartezeit zwischen zwei Verbindungsaufbauversuchen (retryDelay) (optional)	Array [1..16] von Integer (0..86400)	Fehlt dieser optionale Parameter, wird der Standardwert verwendet. (Standardwert: 5) Legt die Wartezeit zwischen zwei Verbindungsaufbauversuchen fest (in Sekunden). Der erste Listeneintrag bestimmt die Wartezeit zwischen Versuch 1 und Versuch 2. Der zweite zwischen Versuch 2 und Versuch 3, usw. Die maximale Anzahl von Einträgen wird vom GWH im ICS beschrieben. Sind weniger Einträge als maxRetryCount vorhanden, wird der letzte Eintrag für die weiteren Runden verwendet.
Konfigurationsparameter für Vorhaltefristen der Rolle CON		
Maximale Speicherdauer von Einträgen im Anschlussnutzer-Log "userId" (maxLogDuration) (optional)	Integer (1..13140)	Wird dieser optionale Parameter für die Rolle CON beim Import nicht angegeben, dann wird der vom Hersteller angegebene Standardwert gemäß Vorhaltefrist angenommen. (Standardwert: 465) Dieser Parameter hat nur eine Bedeutung für das Anschlussnutzer-Log der Rolle CON. Die maximale Zeit (in Tagen) für die Speicherdauer von Einträgen im Anschlussnutzer-Log.
Erweiterungen (extensions) (optional)	Any	Ist dieser optionale Parameter vorhanden, kann der GWA herstellerspezifische Erweiterungen zur Verbindungsherstellung übergeben, die im SMGW persistiert werden. Für die herstellerspezifischen Erweiterungen ist das Default-Verhalten des SMGW zu beschreiben, sofern dieser Parameter nicht vorhanden ist. Damit soll gewährleistet werden, dass das SMGW auch mit GWA-Systemen interoperabel ist, die die Erweiterungen nicht unterstützen. Siehe auch ▸ICS.HAN.Kommunikationsprofile.10.

Tabelle 3.83 Parameter des Profils "HAN-Kommunikationsprofil" (hanCommunicationProfile)

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

Implementation Conformance Statements



ICS.HAN.Kommunikationsprofile.10

Der GWH **MUSS** im ICS erklären, ob das SMGW das Datenfeld Erweiterungen im HAN-Kommunikationsprofil verarbeitet. In diesem Fall muss der GWH das Verhalten des SMGW beschreiben, sofern Datenfelder mit herstellerspezifischen Erweiterungen des SMGW nicht vorhanden sind.

3.22.23 Schlüsselreferenzen

Diese Datenstruktur enthält als Rückgabeparameter die Schlüsselreferenzen im der SMGW- und Root-CA Schlüssel im Sicherheitsmodul.

Datenfeld / Parameter	Datentyp	Beschreibung
TLS-Schlüsselobjektreferenz (tlsKeyRef) (optional)	String (hexString)	Dieses optionale Datenfeld ist nur als Rückgabeparameter in FA.DoPrepareImportGwaKeys vorhanden. Schlüsselobjekt-Referenz für TLS-Schlüssel
ENC-Schlüsselobjektreferenz (encKeyRef) (optional)	String (hexString)	Dieses optionale Datenfeld ist nur als Rückgabeparameter in FA.DoPrepareImportGwaKeys vorhanden. Schlüsselobjekt-Referenz für Verschlüsselungs-Schlüssel
SIG-Schlüsselobjektreferenz (sigKeyRef) (optional)	String (hexString)	Dieses optionale Datenfeld ist nur als Rückgabeparameter in FA.DoPrepareImportGwaKeys vorhanden. Schlüsselobjekt-Referenz für Signatur-Schlüssel
AUT-Schlüsselobjektreferenz (autKeyRef) (optional)	String (hexString)	Dieses optionale Datenfeld ist nur als Rückgabeparameter in FA.DoPrepareImportGwaKeys vorhanden. Schlüsselobjekt-Referenz für Authentifizierungs-Schlüssel
ROOTCA-Schlüsselobjektreferenz (rootCaKeyRef) (optional)	String (hexString)	Dieses optionale Datenfeld ist nur als Rückgabeparameter in FA.DoPrepareImportRootCaKey vorhanden Schlüsselobjekt-Referenz für Root-CA-Schlüssel

Tabelle 3.84 Datenfelder / Parameter des Datenobjekts "Schlüsselobjektreferenzen" (keyRefSet)

3.22.24 LMN-Schnittstellenkonfigurationsprofil

LMN-Schnittstellenkonfigurationsprofile legen die Parameter für die Konfiguration einer LMN-Schnittstelle des SMGW fest.

LMN-Schnittstellenkonfigurationsprofile werden im SMGW persistiert.

Parameter	Datentyp	Beschreibung
Profil-ID (profileId)	String (name)	Der im SMGW eindeutige Bezeichner des LMN-Schnittstellenkonfigurationsprofils.
Schnittstellenbezeichnung (ifName)	String (name)	Im SMGW eindeutige Bezeichnung der physischen LMN-Schnittstelle. Beginnt mit "LMN" LMN1 für die bedrahtete RS-485/HDLC Schnittstelle LMN2 für die drahtlose SRD 868MHz Schnittstelle (EN13737-4)
Erweiterungen (extensions) (optional)	Any	Ist dieser optionale Parameter vorhanden, kann der GWA herstellerspezifische Erweiterungen zur Verbindungsherstellung übergeben, die im SMGW persistiert werden. Für die herstellerspezifischen Erweiterungen ist das Default-Verhalten des SMGW zu beschreiben, sofern dieser Parameter nicht vorhanden ist. Damit soll gewährleistet werden, dass das SMGW auch mit GWA-Systemen interoperabel ist, die die Erweiterungen nicht unterstützen.

Tabelle 3.85 Parameter des Profils "LMN-Schnittstellenkonfigurationsprofil" (lmnIfProfile)

Das SMGW kann im Datenfeld "Erweiterungen" weitere Parameter für Schnittstellenkonfigurationsprofile unterstützen.

Implementation Conformance Statements



ICS.LMN.IfProfile.10

Der GWH **MUSS** im ICS erklären, ob das SMGW das Datenfeld Erweiterungen im LMN-Schnittstellenkonfigurationsprofil verarbeitet. In diesem Fall muss der GWH das Verhalten des SMGW beschreiben, sofern Datenfelder mit herstellerspezifischen Erweiterungen des SMGW nicht vorhanden sind.

3.22.25 LMN-Kommunikationsprofil (Zählerprofil)

Ein LMN-Kommunikationsprofil beschreibt die Konfiguration für das SMGW, die notwendig ist, um mit einer Messeinrichtung zu kommunizieren.

Parameter	Datentyp	Beschreibung
Profil-ID (meterId)	String (huid)	Dieses Datenfeld identifiziert das Profil anhand des eindeutigen Bezeichners der Messeinrichtung auf Anwendungsebene im SMGW. Dieses Datenfeld dient als Ressourcen-Identifikation.
Messwertempfang aktiviert (active) (optional)	Boolean	Ist dieser optionale Parameter nicht vorhanden, wird der Standardwert angenommen. (Standardwert: true) Wird dieser Parameter auf "false" gesetzt werden empfangene Messwertnachrichten ignoriert (nicht verarbeitet) und keine Anfragen an bedrahtet kommunizierende Messeinrichtungen gestellt.
Geräte-Adresse (address) (optional)	String (hexString)	Wird dieser optionale Parameter nicht angegeben, dann wird die Adresse über die Geräte-ID bestimmt. Sofern für die Kommunikation mit der Messeinrichtung erforderlich, kann der GWA die Kommunikationsadresse der Messeinrichtung im LMN konfigurieren.
Kommunikationsszenario (ks)	Enumeration • LKS1 • LKS2	Dieser Parameter legt das Kommunikationsszenario zur Kommunikation mit der Messeinrichtung fest. Siehe auch ▸Abschnitt 4.3.2. Die Wertebelegungen haben folgende Bedeutung: • LKS1: beschreibt die bidirektionale bedrahtete Kommunikation mit den Protokollen des LKS1. • LKS2: beschreibt die unidirektionale drahtlose Kommunikation mit den Protokollen des LKS2.
Kommunikationsschlüssel (pairingKey) (optional)	String (hexString)	Ist dieses optionale Datenfeld nicht vorhanden, erfolgt die kommunikative Anbindung von bidirektional kommunizierenden Zählern mittels initialem Kommunikationszertifikat des Zählers. Dieser Parameter enthält den für die (initiale) kommunikative Anbindung der Messeinrichtung verwendeten (initialen) Schlüssel, der für die Absicherung der Kommunikation mit dem Zähler verwendet wird. 16-Byte Zeichenfolge (Symmetrischer Schlüssel, nicht auslesbar). Beim Auslesen des Profils ist dieser Parameter nicht vorhanden.
Kommunikationszertifikat des Zählers (mtrTlsCert) (optional)	String (hexString)	Ist dieses optionale Datenfeld nicht vorhanden, erfolgt die kommunikative Anbindung von bidirektional kommunizierenden Zählern mittels initialem symmetrischen Schlüssel des Zählers. Der Wert des Parameters ist davon abhängig, ob es sich um ein einzuspielendes oder ein ausgelesenes Profil handelt. Beim Einspielen: Das für die (initiale) kommunikative Anbindung der Messeinrichtung verwendete TLS-Zertifikat der Messeinrichtung Beim Auslesen: Das vom SMGW aktualisierte MTR_LMN_TLS_CRT der Messeinrichtung.
Vertrauensanker des SMGW (smgwTlsCert) (optional)	String (hexString)	Dieser Parameter ist nur beim Auslesen des Profils vorhanden. Der Wert des Parameters ist davon abhängig, ob es sich um ein einzuspielendes oder ein ausgelesenes Profil handelt. Beim Einspielen: nicht vorhanden Beim Auslesen: Das vom SMGW an die Messeinrichtung exportierte GW_LMN_TLS_CRT.

Parameter	Datentyp	Beschreibung
Wandlerfaktor I (currentTransformerRatio) (optional)	Integer (1..60000)	Ist dieses Datenfeld nicht vorhanden, ist kein Wandler vorhanden bzw. der Wandlerfaktor ist 1.0 (Standardwert: 1.0) Dieser optionale Parameter wird nur angegeben, wenn die Messeinrichtung mit einem Messwandler für den Strompfad betrieben wird. Dieser Parameter enthält den Faktor des Messwandlers für den Strompfad I. Beispiel: Ein Wert 20.0 bedeutet, dass der Wandler einen Strom von 100A zu einem Strom von 5A an der Messeinrichtung umsetzt. Der Parameter wird nicht zur Berechnung im SMGW verwendet. Er wird vom MSB zur Verwendung durch den Anschlussnutzer/Anlagenbetreiben konfiguriert. Die Bereitstellung erfolgt über das der Messeinrichtung zugeordnete Auswertungsprofil.
Wandlerfaktor U (voltageTransformerRatio) (optional)	Integer (1..60000)	Ist dieses Datenfeld nicht vorhanden, ist kein Wandler vorhanden bzw. der Wandlerfaktor ist 1.0 Dieser optionale Parameter wird nur angegeben, wenn die Messeinrichtung mit einem Messwandler für Spannungspfad betrieben wird. Dieser Parameter enthält den Faktor des Messwandlers für den Spannungspfad U. Beispiel: Ein Wert 100.0 bedeutet, dass der Wandler eine Spannung von 10.000V zu einer Spannung von 100V an der Messeinrichtung umsetzt. Der Parameter wird nicht zur Berechnung im SMGW verwendet. Er wird vom MSB zur Verwendung durch den Anschlussnutzer/Anlagenbetreiber konfiguriert. Die Bereitstellung erfolgt über das der Messeinrichtung zugeordnete Auswertungsprofil.
Unterstützte OBIS-Kennzahlen (supportedValues)	Array [0..100] von String (obis)	Dieser Parameter gibt an, welche OBIS-Kennzahlen von der Messeinrichtung geliefert bzw. abgefragt werden können.
Erweiterungen (extensions) (optional)	Any	Ist dieser optionale Parameter vorhanden, kann der GWA herstellerspezifische Erweiterungen zur Kommunikation mit der Messeinrichtung übergeben, die im SMGW persistiert werden. Für die herstellerspezifischen Erweiterungen ist das Default-Verhalten des SMGW zu beschreiben, sofern dieser Parameter nicht vorhanden ist. Damit soll gewährleistet werden, dass das SMGW auch mit GWA-Systemen interoperabel ist, die die Erweiterungen nicht unterstützen. Siehe auch ▸ICS.MWV.Zählerprofil.10.

Tabelle 3.86 Parameter des Profils "LMN-Kommunikationsprofil" (lmnComProfile)

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

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

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

Implementation Conformance Statements



ICS.MWV.Zählerprofil.10

Der GWH **MUSS** im ICS erklären, ob das SMGW das Datenfeld Erweiterungen verarbeitet. In diesem Fall muss der GWH das Verhalten des SMGW beschreiben, sofern Datenfelder mit herstellerspezifischen Erweiterungen des SMGW nicht vorhanden sind.

3.22.26 Logbuch und Ereignisse

Die Logbuch-Datenstruktur dient der Ausgabe von Logbüchern (Syslog, Eichlog, Userlog).

Logbuch-Datenstruktur

Datenfeld	Datentyp	Beschreibung
Profil-ID (profileId)	String (name)	Dieses Datenfeld identifiziert das Logbuch unter allen Logbüchern an den Schnittstellen des SMGW eindeutig. Für ein Logbuch vom Typ USER enthält das Datenfeld die eindeutige Kennung des Anschlussnutzers (userId) und bestimmt darüber den Anschlussnutzer, der zur Einsicht der Daten berechtigt ist. Für ein Logbuch vom Typ CAL oder SYS enthält das Datenfeld die SMGW-ID. Dieses Datenfeld dient als Ressourcen-Identifikation.
Typ des Logbuchs (logType)	Enumeration • SYS • CAL • USER	Identifiziert den Typ des Logbuches. Die Wertebelegungen haben folgende Bedeutung: • SYS: Systemlog für GWA und Servicetechniker. • CAL: Eichlog für die Stelle zur Befundprüfung und Konformitätsbewertung. • USER: Anschlussnutzerlog (auch UserLog) für Endkunden.
List von Logbucheinträgen (events)	Array [0..n] von Tupel	Eine chronologisch (absteigend) sortierte Liste von Ereignissen. Das neuste Ereignis wird zuerst übertragen.
In diesem Datenfeld ist ein Logergeignis enthalten. Folgende Elemente sind an dieser Stelle möglich: • Event (definiert in ▸Tabelle 3.88)		

Tabelle 3.87 Datenfelder des Datenobjekts "Logbuch" (logbook)

Logbuch-Eintrag

Ein Logeintrag (Event) enthält den Zeitpunkt eines Ereignisses, die Identifikation des Ereignisses und Informationen zum Ereignis.

Datenfeld	Datentyp	Beschreibung
Laufende Nummer (idx)	Integer (1..n)	Seit Erzeugung des individuellen Logbuches für jeden geschriebenen Logbuch-Eintrag inkrementierte Zahl (Erster Eintrag 1). Zur Prüfung der Vollständigkeit exportierter Logbücher und zur Korrelation mit dem System-Log bei GWA-Benachrichtigung.
Zeitstempel des Ereignisses (ts)	String (dateTime)	Zeitpunkt der Protokollierung des Ereignisses (UTC).
Ereignistyp (eventType)	String (name)	Identifiziert den Typ des Ereignis (Vendor.EventId.EventSubId). Siehe auch ▸Tabelle A.1.
Bewertung (level)	Enumeration • I • W • E • F	Bewertung des Ereignisses Die Wertebelegungen haben folgende Bedeutung: • I: Info (erfolgreiche Ausführung) • W: Warning (Anomalie) • E: Error (Abbruch mit Fehler) • F: Fatal (Permanenter Fehlerzustand)
Ereignisparameter (params)	Array [0..10] von String	Indexbasierte Parameter für das Ereignis (Die Position des Parameters in der Reihenfolge bestimmt seine Bedeutung). Siehe auch ▸Tabelle A.1.

Datenfeld	Datentyp	Beschreibung
Erweiterung (extension) (optional)	String	Ist dieses optionale Datenfeld vorhanden, kann der GWH herstellerspezifische Erweiterungen zum Ereignis angeben. Herstellerspezifische Ergänzung des Ereignisses. Für die herstellerspezifischen Erweiterungen ist deren Bedeutung zu beschreiben. Sofern dieses optionale Datenfeld vorhanden ist, darf es die Bedeutung der Ereignisse nicht verändern. Siehe auch ▸ICS.FAKAT.SmgwMonitoring.31.

Tabelle 3.88 Datenfelder des Datenobjekts "Ereignis" (event)

Das SMGW **KANN** im Datenfeld für Erweiterungen weitere Datenfelder für Ereignisse unterstützen. ▸ICS.FAKAT.SmgwMonitoring.31 [REQ.FAKAT.SmgwMonitoring.31]



ICS.FAKAT.SmgwMonitoring.31

Der GWH **MUSS** im ICS erklären, ob das SMGW das Datenfeld "Erweiterungen" im Ereignis übermittelt.



ICS.FAKAT.SmgwMonitoring.32

Sofern das SMGW das Datenfeld "Erweiterungen" übermittelt, **MUSS** der GWH im ICS die Bedeutung der Erweiterung beschreiben.

Ereignisliste für Benachrichtigungen

Eine Ereignisliste (▸Tabelle 3.89) enthält mindestens ein Ereignis, das bei einer Benachrichtigung an den Empfänger (GWA) übermittelt wird.

Datenfeld	Datentyp	Beschreibung
Ereignisliste (events)	Array [0..n] von Tupel	Eine chronologisch (absteigend) sortierte Liste von Ereignissen. Das auslösende Ereignis wird zuerst übertragen.
In diesem Datenfeld ist ein Ereignis enthalten. Folgende Elemente sind an dieser Stelle möglich: • Event (definiert in ▸Tabelle 3.88)		

Tabelle 3.89 Datenfelder des Datenobjekts "Ereignisliste" (eventList)

3.22.27 Parameter zum Verkürzen von Logs

Diese Datenstruktur beschreibt die Mindestanforderungen an den Parametersatz zur Verkürzung von Logs.

Parameter	Datentyp	Beschreibung
Zeitpunkt vor dem die Logbucheinträge gelöscht werden können (truncationDateTime)	String (dateTime)	Die vor dem in diesem Parameter angegebenen Zeitpunkt zeitgestempelten Logbucheinträge sollen gelöscht werden.
Identifikation des Anschlussnutzer-Logs (userId) (userId) (optional)	String (name)	Dieser optionale Parameter ist nur vorhanden, wenn das Anschlussnutzer-Log durch den GWA verkürzt werden soll. Identifiziert das Anschlussnutzer-Log über die "userId"

Tabelle 3.90 Parameter des Profils "Aufrufparameter zur Logbuchverkürzung" (logTruncParameters)

3.22.28 Messgerätestatus

Diese Datenstruktur beschreibt die Bedeutung von Statusinformationen der Messeinrichtung und wird aus anderen Datenstrukturen an geeigneter Stelle referenziert.

Datenfeld	Datentyp	Beschreibung
Statuswort (statusWord)	String (hexString)	Das Datenfeld enthält das 32 Bit Statuswort der Messeinrichtung gemäß gemeinsamer Festlegung von DVGW, VDE/DKE/FNN und OMS. Die niederwertigen Bits 0-7 kennzeichnen den Typ (Herkunft) des Statusworts. Die Bits 8-31 signalisieren gemäß Statusworttyp die Informationen (Warnungen, Fehler, Status).

Tabelle 3.91 Datenfelder des Datenobjekts "Messgerätestatus" (meterStatus)

3.22.29 Zählerstatusliste

Diese Datenstruktur listet die im SMGW identifizierten, kommunikativ erreichbaren Zähler auf.

Datenfeld	Datentyp	Beschreibung
Zähler (meter)	Array [0..n] von Tupel	Enthält die Liste der Zählerstatuseinträge
Messgeräteidentifikation (meterId)	String (huid)	Dieses Datenfeld identifiziert die Messeinrichtung anhand des eindeutigen Bezeichners der Messeinrichtung auf Anwendungsebene gemäß [DIN43849] im SMGW.
Linklayer-Kommunikationsadresse (l2Address) (optional)	String (hexString)	Dieses optionale Datenfeld ist nur vorhanden, wenn eine Adresse ausgegeben werden kann. Dieses Datenfeld enthält die Kommunikationsadresse der Messeinrichtung auf dem OSI Layer 2 (Bspw. eine Layer 2 HDLC oder DLL Adresse).
Netzwerklayer-Kommunikationsadresse (l3Address) (optional)	String (hexString)	Dieses optionale Datenfeld ist nur vorhanden, wenn eine Adresse ausgegeben werden kann. Dieses Datenfeld enthält die Kommunikationsadresse der Messeinrichtung auf dem OSI Layer 3.
Kommunikationsszenario (ks) (optional)	Enumeration • LKS1 • LKS2 • LMN	Dieses optionale Datenfeld ist nur vorhanden, wenn das Kommunikationsszenario ausgegeben werden kann. Bezeichnet das Kommunikationsszenario, über das der Zähler kommunikativ erreichbar ist. LMN bezeichnet eine herstellerspezifische LMN-Anbindung.
Empfangsfeldstärke (rssi) (optional)	Integer (-100..0)	Dieses optionale Datenfeld ist nur vorhanden, wenn eine Empfangsfeldstärke ausgegeben werden kann. Gibt die Empfangsfeldstärke (dB) der drahtlos kommunizierenden Messeinrichtung an (negativer Wert).
Letzter Empfangszeitpunkt (lastTs) (optional)	String (dateTime)	Ist dieses optionale Datenfeld nicht vorhanden, wurde keine Nachricht vom Zähler empfangen. Dieses Datenfeld enthält den letzten Empfangszeitpunkt einer Nachricht von der Messeinrichtung.
Kommunikativer Anbindungsstatus (pairingState)	Enumeration • PROFILE_ONLY • IDENTIFIED • AUTHENTICATED • DATA_EXCHANGE	Dieses Datenfeld enthält Informationen über den Anbindungsstatus des Zählers. Die Wertebelegungen haben folgende Bedeutung: • PROFILE_ONLY: kennzeichnet den Zustand, wenn ein LMN-Kommunikationsprofil konfiguriert ist, ohne dass die Messeinrichtung im Netzwerk identifiziert wurde. • IDENTIFIED: kennzeichnet den Zustand, wenn eine Messeinrichtung über eine Kommunikationsadresse erreichbar ist und noch kein Pairing über den Kommunikationsschüssel erfolgt ist. Da der Zähler nicht authentifiziert ist, werden Listeneinträge mit diesem Anbindungsstatus nach wenigen Stunden aus der Liste entfernt. • AUTHENTICATED: kennzeichnet den Zustand, wenn das Pairing mit dem Kommunikationsschlüssel erfolgt ist, aber noch keine Messwertnachricht entschlüsselt wurde. • DATA_EXCHANGE: kennzeichnet den Zustand, wenn mindestens eine empfangene Nachricht erfolgreich entschlüsselt wurde.

Datenfeld	Datentyp	Beschreibung
Erweiterungen (extensions) (optional)	Any	Ist dieser optionale Parameter vorhanden, kann der GWH herstellerspezifische Erweiterungen zum Zustand der kommunikativen Anbindung des Zählers ausgeben. Dieses Datenfeld enthält herstellerspezifische Statusinformationen zum Zustand der kommunikativen Anbindung des Zählers.

Tabelle 3.92 Datenfelder des Datenobjekts "Zählerstatusliste" (meterStatusList)

3.22.30 Netzwerkdiagnose-Konfigurationsprofil

Profil zur Parametrierung des Versands von Netzwerkdiagnosedaten an einen autorisierten externen Marktteilnehmer (EMT) oder den GWA.

Parameter	Datentyp	Beschreibung
Profil-ID (profileId)	String (name)	Dieses Datenfeld identifiziert das NDS-Konfigurationsprofil unter allen NDS-Konfigurationsprofilen an den Schnittstellen des SMGW eindeutig. Dieses Datenfeld wird als Ressourcen-Identifikation verwendet.
Physische Schnittstelle (physInterface)	String	Eindeutige Identifikation der physischen Schnittstelle, für die ein Versand von Netzwerkdiagnosedaten durchgeführt werden soll.
WAN-Kommunikationsprofil (referencedCommunicationProfile)	String (name)	Enthält den eindeutigen Bezeichner des WAN-Kommunikationsprofils, das zum Versand verwendet werden soll.
Übertragene Attribute (transferredAttributes)	Array [0..n] von String (name)	Liste von Attributnamen zur Auswahl der zu versendenden Netzwerkdiagnosedaten. Mögliche Werte sind unter anderem "rssi", "snr" oder "imei" sowie weitere vom Hersteller des SMGW festgelegte Attributnamen. Siehe auch ▸Abschnitt 3.22.31.
Übertragungsintervall Normal (intervalPeriodic) (optional)	Integer (0..n)	Wenn der Parameter nicht angegeben ist, wird der Standardwert angenommen. (Standardwert: 0) Legt das zu verwendende Versandintervall in Sekunden im Normalfall (keine Schwellwertverletzung, nicht nach dem Start des SMGW) fest. Der Wert 0 deaktiviert den periodischen Versand.
Übertragungsintervall Systemstart (intervalStart) (optional)	Integer (0..n)	Wenn der Parameter nicht angegeben ist, wird der Standardwert angenommen. (Standardwert: 0) Legt das zu verwendende Versandintervall in Sekunden nach einem SMGW Neustart fest. Wenn der Parameter angeben ist, dann muss auch der Parameter "durationStart" angegeben sein. Wenn der Wert 0 ist, findet kein periodischer Versand im Zeitraum nach dem Neustart statt. Dies bezieht sich nur auf den periodischen Versand mit abweichendem Intervall. Der periodische Versand nach "intervalPeriodic" findet, sofern angegeben, statt.
Dauer Systemstartzustand (durationStart) (optional)	Integer (0..n)	Wenn der Parameter nicht angegeben ist, wird der Standardwert angenommen. (Standardwert: 0) Legt die Dauer in Sekunden nach dem Startvorgang des SMGW fest, für die "intervalStart" zur Bestimmung der Versandzeitpunkte verwendet wird. Wenn der Parameter angeben ist, dann muss auch der Parameter "intervalStart" angegeben sein. Wenn der Wert 0 ist, findet kein periodischer Versand im Zeitraum nach dem Neustart statt.
Schwellwerte (thresholds) (optional)	Array [0..n] von Tupel	Wenn dieser optionale Parameter nicht vorhanden ist, dann findet kein Versand aufgrund von Schwellwertverletzungen statt. Liste von Schwellwertdefinitionen mit folgenden Parametern.

Parameter	Datentyp	Beschreibung
Attributname (attributName)	String (name)	Eindeutiger Attributname, der ein Netzwerkdiagnosedatum identifiziert. Der Attributname muss in "transferedAttributes" vorhanden sein.
Schwellwert (threshold)	Integer (-n..m)	Festlegung eines numerischen Werts, dessen Unter- oder Überschreiten eine Schwellwertverletzung darstellt.
Schwellwert ist Obergrenze (upperLimit)	Boolean	Dieser Parameter legt fest, ob eine Schwellwertverletzung bei Überschreiten (True) oder bei Unterschreiten (False) des Werts in "threshold" vorliegt.
Versandintervall nach Schwellwert (intervalThreshold) (optional)	Integer (0..n)	Wenn der Parameter nicht angegeben ist, wird der Standardwert angenommen. (Standardwert: 0) Legt das zu verwendende Versandintervall in Sekunden nach dem Auftreten einer Schwellwertverletzung fest, wenn der Parameter nicht angegeben ist. Beim Wert 0 findet kein abweichender periodischer Versand im Zeitraum nach einer Schwellwertverletzung statt.
Dauer nach Schwellwert (durationThreshold) (optional)	Integer (0..n)	Wenn der Parameter nicht angegeben ist, wird der Standardwert angenommen. (Standardwert: 0) Legt die Mindestdauer in Sekunden nach dem Auftreten einer Schwellwertverletzung fest, für die "intervalThreshold" zur Bestimmung der Versandzeitpunkte verwendet werden soll. Wenn der Parameter angeben ist, dann muss auch der Parameter "intervalThreshold" angegeben sein. Bei einem Wert von 0, wird "intervalThreshold" solange verwendet, bis keine Schwellwertverletzung mehr vorliegt.
Erweiterungen (extensions) (optional)	Any	Ist dieser optionale Parameter vorhanden, kann der GWA herstellerspezifische Erweiterungen zur Konfiguration des Netzwerkdiagnoseservice übergeben, die im SMGW persistiert werden. Für die herstellerspezifischen Erweiterungen ist das Default-Verhalten des SMGW zu beschreiben, sofern dieser Parameter nicht vorhanden ist. Damit soll gewährleistet werden, dass das SMGW auch mit GWA-Systemen interoperabel ist, die die Erweiterungen nicht unterstützen. Siehe auch ▸ICS.FAKAT.NetworkDiagnosis.10.

Tabelle 3.93 Parameter des Profils "Netzwerkdiagnose-Konfigurationsprofil" (ndsConfigurationProfile)

Das SMGW **KANN** im Datenfeld "Erweiterungen" weitere Parameter für Netzwerkdiagnoseprofile unterstützen. [REQ.FAKAT.NetworkDiagnosis.30]

Implementation Conformance Statements



ICS.FAKAT.NetworkDiagnosis.10

Der GWH **MUSS** im ICS erklären, ob das SMGW das Datenfeld Erweiterungen im Netzwerkdiagnoseprofil verarbeitet. In diesem Fall muss der GWH das Verhalten des SMGW beschreiben, sofern Datenfelder mit herstellerspezifischen Erweiterungen des SMGW nicht vorhanden sind.

3.22.31 Zulässige Netzwerkdiagnose-Attribute

Netzwerkdiagnosedatum	Attributname	Datentyp	Beschreibung
Received signal strength indication (RSSI)	"rssi"	Number	Gleitkommazahl in dBm ohne negatives Vorzeichen. Indikator für die Empfangsfeldstärke (Gesamtsignal).
Reference signal received power (RSRP)	"rsrp"	Number	Gleitkommazahl in dBm ohne negatives Vorzeichen. Indikator für die LTE Empfangsfeldstärke (Nutzsignal).

Netzwerkdiagnosedatum	Attributname	Datentyp	Beschreibung
Reference Signal Received Quality (RSRQ)	"rsrq"	Number	Gleitkommazahl in dB ohne negatives Vorzeichen. Indikator für die LTE Empfangsqualität.
Signal-to-noise ratio (SNR)	"snr"	Number	Gleitkommazahl in dB. Indikator für die Signalqualität.
Mobile country code (MCC)	"mcc"	Integer (0..999)	Länderkennung des verwendeten Mobilfunknetzwerks.
Mobile network code (MNC)	"mnc"	Integer (0..9999)	Zusammen mit dem MCC eindeutige Identifikation des Funknetzanbieters des verwendeten Mobilfunknetzwerks.
Provider	"provider"	String	Name des verwendeten Mobilfunkproviders.
Cell ID (CID) der verwendeten Basisstation	"cid"	Text	Eindeutige Identifikation der derzeit verwendeten Basisstation.
Technologie	"technology"	String	Verwendete Medientechnologie (z.B. Ethernet, LTE).
Betriebsart	"mode"	String	Betriebsart der verwendeten Technologie (z.B. 100Base-TX).
Frequenzband	"band"	String	Derzeit verwendetes Frequenzband.
International Mobile Equipment Identity (IMEI)	"imei"	String (15)	Enthält nur die Ziffern 0-9. Eindeutige Seriennummer zur Identifikation des Mobilfunkmodems.
International Mobile Subscriber Identity (IMSI)	"imsi"	String (6..15)	Enthält nur die Ziffern 0-9. International eindeutige Mobilfunkteilnehmerkennung.
Integrated Circuit Card Identifier (ICC-ID)	"iccid"	String	Eindeutige Nummer der SIM-Karte.
Geräteadresse	"linkaddress"	String	Adresse des medienabhängigen Link-Layers (z.B. MAC-Adresse).
Netzwerkprotokoll	"protocol"	String	Verwendetes Netzwerkprotokoll (z.B. IPv4, IPv6).
IPv4 Adresse	"ipv4"	String	In Dotted-Decimal Notation mit Slash-Notation für Subnetzmaske. Derzeit verwendete IPv4 Adresse des SMGW.
IPv6 Adressen	"ipv6addresses"	Array von String	Derzeit verwendete IPv6 Adressen des SMGW mit Slash-Notation für Präfixlänge.
Betriebszeit der Schnittstelle	"ifuptime"	Integer	Nicht-negative Ganzzahl in Sekunden. Betriebszeit der physischen Schnittstelle des SMGW.
Erfolgreiche Einbuchungen	"successnetlogin"	Integer	Nicht-negative Ganzzahl. Anzahl erfolgreicher Einbuchungen bei einem Provider seit letztem Neustart.
Erfolglose Einbuchungen	"failednetlogin"	Integer	Nicht-negative Ganzzahl. Anzahl erfolgloser Einbuchungen bei einem Provider seit letztem Neustart.
Übertragenes Datenvolumen (gesendet)	"tx"	Integer	Nicht-negative Ganzzahl in Bytes. Gesendetes Datenvolumen seit letztem Neustart.
Übertragenes Datenvolumen (empfangen)	"rx"	Integer	Nicht-negative Ganzzahl in Bytes. Empfangenes Datenvolumen seit letztem Neustart.
Frame Statistik	"frametraffic"	Tupel von (Integer, Integer)	Zusammenfassende Historie der ein- und ausgehenden Protocol Data Units des Link-Layers.
Paket Statistik	"packettraffic"	Tupel von (Integer, Integer)	Zusammenfassende Historie der ein- und ausgehenden Protocol Data Units des Network-Layers.
Bit Error Rate	"ber"	Number	Gleitkommazahl in Prozent. Aktuell gemessene Bitfehlerrate des Physiscal Layers. Die Zeitdauer, auf die sich die Messung bezieht, wird vom GWH beschrieben.

Netzwerkdiagnosedatum	Attributname	Datentyp	Beschreibung
Round Trip Time	"rtt"	Integer	Positive Ganzzahl in ms. Aktuell gemessene Rundlaufzeit (Summe aus Up- und Downstream Latenz) des Link-Layers.

Tabelle 3.94 Zulässige Netzwerkdiagnosedaten

3.22.32 Netzwerkdiagnose-Statusprofil

Welche Attribute übertragen werden, wird über das Netzwerkdiagnose-Konfigurationsprofil (Siehe ▸Abschnitt 3.22.30) festgelegt.

Datenfeld	Datentyp	Beschreibung
NDS-Konfigurationsprofil-Referenz (profileRefId) (optional)	String (name)	Ist dieses optionale Datenfeld nicht vorhanden, wurden die Statusinformationen ohne Bezug zu einem NDS-Konfigurationsprofil erzeugt. Beispielsweise durch Abfrage des GWA oder Servicetechnikers. Dieses Datenfeld identifiziert das NDS-Konfigurationsprofil, dem diese Statusinformationen zugeordnet sind.
Geräte-ID (deviceId)	String (huid)	Dieses Datenfeld identifiziert das Gerät, dem die Netzwerkdiagnosedaten zugeordnet sind.
Physische Schnittstelle (physInterface)	String (name)	Eindeutige Identifikation der physischen Geräte-Schnittstelle, der die Netzwerkdiagnosedaten zugeordnet sind.
Zeitpunkt der Erstellung (creationTime)	String (dateTime)	Zeitpunkt, zu dem die Datenstruktur erstellt wurde.
Werte der Netzwerkdiagnosedaten (data)	Array [0..n] von Tupel	Schlüssel-Werte-Paare aller im Konfigurationsparameter "Übertragene Netzwerkdiagnosedaten" festgelegten Netzwerkdiagnosedaten. Vom GWH zusätzlich implementierte Attributnamen-Werte-Paare werden innerhalb von "additionalData" übermittelt.
Attribut (attr)	String (name)	Name des Attributs. Siehe auch ▸Abschnitt 3.22.31.
Wert (value)	Any	Wert des Attributs. Der Datentyp des Werts ist abhängig vom jeweiligen Attribut. Siehe auch ▸Abschnitt 3.22.31.
Weitere Daten (additionalData) (optional)	Any	Ist dieses optionale Datenfeld vorhanden, kann der GWH weitere Daten im Rahmen des Versands von Netzwerkdiagnosedaten übermitteln. Attributnamen-Werte-Paare von Netzwerkdiagnosedaten, die vom SMGW über die Auflistung in "data" hinaus versandt werden.

Tabelle 3.95 Datenfelder des Datenobjekts "Netzwerkdiagnose-Statusprofil" (ndsStatusProfile)

Aufgrund verschiedener Technologien und Modem-Implementierungen können weitere Netzwerkdiagnosedaten vorhanden sein oder andere Begriffe verwendet werden. Das SMGW **KANN** den Versand weiterer Netzwerkdiagnosedaten unter Berücksichtigung von ▸ICS.FAKAT.NetworkDiagnosis.20 unterstützen. [REQ.FAKAT.NetworkDiagnosis.70]

Implementation Conformance Statements



ICS.FAKAT.NetworkDiagnosis.20

Der GWH **MUSS** eine Liste **aller** Netzwerkdiagnosedaten bereitstellen, die das SMGW versenden kann. Für alle Netzwerkdiagnosedaten, die nicht in ▸Abschnitt 3.22.31 gelistet sind, **MUSS** der Hersteller des SMGW zusätzlich eine Beschreibung bereitstellen und begründen, dass die Vertraulichkeit keines Assets des SMGW nach [PP-0073] verletzt wird.

3.22.33 Nicht-validierte Messwerte und nicht-validierte Messwertliste (NWL)

Der Begriff "nicht-validierter Messwert" beschreibt einen Messwert, der ohne Überprüfung von Fehlergrenzen übermittelt wird. Ein Bezug zu Registrierzeitpunkten ist nicht erforderlich. Die Datenstruktur übermittelt eine Liste aller zu einem Messzeitpunkt erfassten Messwerte.

3.22.33.1 NWL

Datenfeld	Datentyp	Beschreibung
Messgeräteidentifikation (meterId)	String (huid)	Dieses Datenfeld enthält die herstellerübergreifende Identifikationsnummer der Messeinrichtung, die Ursprung der Messwerte in dieser NWL ist.
Auswahl des TAF (tafType)	Enumeration • TAF9 • TAF10 • TAF14	Dieses Datenfeld enthält den Typ des Anwendungsfalls, der für die Bildung der Messwertliste herangezogen wurde.
Spalten (columns)	Array [0..n] von Tupel	Spaltenüberschriften für die "Messwerte (values)" der enthaltenen "Messwertliste (meterReadings)". Siehe auch ▸Abschnitt 3.22.3.
OBIS-Kennzahl (obis)	String (obis)	Dieses Datenfeld identifiziert das Medium, die Messgröße und die Messart des zugehörigen Messwerts.
Einheit (unit)	String (0..5)	Dieses Datenfeld beschreibt die Einheit des zugehörigen Messwerts. Der zu verwendende Wert ist abhängig von der oben angegebenen OBIS-Kennzahl. Siehe auch ▸Abschnitt 2.5.2.
Messwertliste (meterReadings)	Array [0..n] von Tupel	Dieses Datenfeld enthält eine Liste von Messwerttupeln in chronologisch steigender Reihenfolge (älteste zuerst), die zu den vom Auswertungsprofil vorgegebenen Zeitpunkten erfasst wurden.
Hierunter befinden sich die nicht-validierten Messwerte. Folgende Elemente sind an dieser Stelle möglich: • NonValidatedReading (definiert in ▸Tabelle 3.97)		

Tabelle 3.96 Datenfelder des Datenobjekts "Nicht-validierte Wertliste (NWL)" (nonValidatedReadingList)

3.22.33.2 Nicht-validierter Messwert

Datenfeld	Datentyp	Beschreibung
Zeitstempel des Messwert-Tupels (ts)	String (dateTime)	Dieses Datenfeld wird aus der Messwertzulieferung übernommen.
Messwerte (values)	Array [0..n] von Tupel	Dieses Datenfeld enthält eine Menge von Messwerten. Wurden keine Messwerte empfangen, dann sind hier keine Messwerte drin enthalten. Weitere Informationen zum Messwert werden über das Datenfeld "Spalten" der übergeordneten NWL festgelegt.
Messwert (value)	Number	Dieses Datenfeld enthält den Messwert
Kombiniertes Statuswort (combinedStatus)	Tupel	Dieses Datenfeld enthält Statusinformationen.
Hierin enthalten sind die Gerätestatusinformationen der Messeinrichtung und des SMGW. Folgende Elemente sind an dieser Stelle möglich: • CombinedStatus (definiert in ▸Tabelle 3.74)		

Tabelle 3.97 Datenfelder des Datenobjekts "Nicht-validierter Messwert" (nonValidatedReading)

3.22.34 Parametersatz für die Auslesung im Bedarfsfall

Diese Datenstruktur beschreibt die Mindestanforderungen an den Parametersatz für die Bedarfsauslesung von Messwerten.

Parameter	Datentyp	Beschreibung
Auswertungsprofil (profileId)	String (name)	Dieses Datenfeld identifiziert das Auswertungsprofil, für das die Bedarfsauslesung ausgelöst werden soll.
Datum des Auslesezeitpunktes (dueDate) (optional)	String (date)	Dieser optionale Parameter ist für FA.OnDemandReading erforderlich. Ist dieser optionale Parameter nicht vorhanden, wird der Vortag angenommen. Für TAF9, TAF10 und TAF14 ist dieser Parameter nicht vorhanden, da immer ein aktueller Wert verschickt wird. Bezeichnet den Ablesetag (in der Vergangenheit). Der Zeitpunkt richtet sich nach dem im Auswertungsprofil festgelegten Tageswechselzeitpunkt (gewöhnlich 24:00:00 MEZ/MESZ).
Berichtszeitraum (reportingPeriod) (optional)	Tupel	Dieser optionale Parameter ist für FA.DoReqExportHistoricReadings erforderlich. Der in der Vergangenheit liegende Zeitraum der nachholend zu übermittelnden Messwerte.
Beginn (from)	String (dateTime)	Dieser Parameter legt den Beginn des Zeitraumes für den Nachholenden Messwertabruf fest.
Ende (to)	String (dateTime)	Dieser Parameter das Ende des Zeitraumes für den Nachholenden Messwertabruf fest.
Erweiterungen (extensions) (optional)	Any	Ist dieser optionale Parameter vorhanden, kann der GWA herstellerspezifische Erweiterungen zur Auslösung der Auslesung im Bedarfsfall übergeben. Für die herstellerspezifischen Erweiterungen ist das Default-Verhalten des SMGW zu beschreiben, sofern dieser Parameter nicht vorhanden ist. Damit soll gewährleistet werden, dass das SMGW auch mit GWA-Systemen interoperabel ist, die die Erweiterungen nicht unterstützen. Siehe auch ▸ICS.FAKAT.MeteringConfig.10.

Tabelle 3.98 Parameter des Profils "Parametersatz für die Auslesung im Bedarfsfall" (onDemandParameters)

Das SMGW **KANN** im Datenfeld "Erweiterungen" weitere Parameter für die Bedarfsauslesung unterstützen. [REQ.FAKAT.MeteringConfig.70]

Implementation Conformance Statements



ICS.FAKAT.MeteringConfig.10

Der GWH **MUSS** im ICS erklären, ob das SMGW das Datenfeld Erweiterungen im Parametersatz zu Auslösung im Bedarfsfall verarbeitet. In diesem Fall muss der GWH das Verhalten des SMGW beschreiben, sofern Datenfelder mit herstellerspezifischen Erweiterungen des SMGW nicht vorhanden sind.

3.22.35 Registrierter Wert und registrierte Wertliste (RWL)

3.22.35.1 Registrierter Wert

Der Begriff "registrierter Wert" beschreibt die Datenstruktur, die im Rahmen der Validierung und Registrierung (▸Registrierung von Messwerten) aus ▸Eingangsmesswerte gebildet wird. Die Datenstruktur ist in ▸Tabelle 3.99 beschrieben. Die Zuordnung zu einer Messeinrichtung wird durch Persistierung innerhalb einer zugehörigen Liste registrierter Werte (▸RWL) hergestellt.

Datenfeld	Datentyp	Beschreibung
Sollregistrierzeitpunkt (refTs)	String (dateTime)	Dieses Datenfeld enthält einen Zeitpunkt im Raster der Registrierperiode, dem der registrierte Wert zugeordnet wird.
Zeitstempel des Messwerts (ts)	String (dateTime)	Dieses Datenfeld wird aus der Messwertzulieferung übernommen.
Messwerte (values)	Array [0..n] von Tupel	Dieses Datenfeld enthält eine Menge von Messwerten. Ist der Gesamtstatus "Fehlender Wert", dann sind hier keine Messwerte drin enthalten. Weitere Informationen zum Messwert werden über das Datenfeld "Spalten" der übergeordneten RWL festgelegt.
Messwert (value)	Number	Dieses Datenfeld enthält den Messwert.
Kombiniertes Statuswort (combinedStatus)	Tupel	Dieses Datenfeld enthält Statusinformationen.
Hierin enthalten sind die Gerätestatusinformationen der Messeinrichtung und des SMGW. Folgende Elemente sind an dieser Stelle möglich: • CombinedStatus (definiert in ▸Tabelle 3.74)		

Tabelle 3.99 Datenfelder des Datenobjekts "Registrierter Messwert" (registeredReading)

3.22.35.2 RWL

Datenfeld	Datentyp	Beschreibung
Messgeräteidentifikation (meterId)	String (huid)	Dieses Datenfeld enthält die herstellerübergreifende Identifikationsnummer der Messeinrichtung, die Ursprung der registrierten Werte in dieser RWL ist.
Registrierperiode (regInterval)	Enumeration • FIVE_MINUTE • QUARTER_HOURLY • HOURLY • DAILY	Die im Auswertungsprofil zu dieser RWL festgelegte Registrierperiode, in der Messwerte in der Liste registriert werden. Die Wertebelegungen haben folgende Bedeutung: • FIVE_MINUTE: 5 minütliche Registrierung zur Verwendung bei Lastgängen. • QUARTER_HOURLY: Viertelstündliche Registrierung zur Verwendung bei elektrischer Energie. • HOURLY: Stündliche Registrierung zur Verwendung bei Gas. • DAILY: Tägliche Registrierung zur Verwendung bei anderen Medien.
Spalten (columns)	Array [0..n] von Tupel	Spaltenüberschriften für die "Messwerte (values)" der enthaltenen "Registrierten Werte (registeredReadings)". Siehe auch ▸Abschnitt 3.22.3.
OBIS-Kennzahl (obis)	String (obis)	Dieses Datenfeld identifiziert das Medium, die Messgröße und die Messart des zugehörigen Messwerts.
Einheit (unit)	String (0..5)	Dieses Datenfeld beschreibt die Einheit des zugehörigen Messwerts. Der zu verwendende Wert ist abhängig von der oben angegebenen OBIS-Kennzahl. Siehe auch ▸Abschnitt 2.5.2.
Registriere Werte (registeredReadings)	Array [0..n] von Tupel	Dieses Datenfeld enthält alle in der RWL persistierten registrierten Werte.
Hierunter befinden sich die registrierten Werte. Folgende Elemente sind an dieser Stelle möglich: • RegisteredReading (definiert in ▸Tabelle 3.99)		

Tabelle 3.100 Datenfelder des Datenobjekts "Registrierte Werteliste (RWL)" (registeredReadingList)

3.22.36 Password-Update Datenstrukturen

Datenstruktur für die Übermittlung des neuen Endkunden-Passwortes.

Parameter	Datentyp	Beschreibung
Passwort (password)	String (6..50)	Dieses Datenfeld enthält das vom Nutzer gewählte neue Passwort.
Passwort Wiederholung (passwordRepeat)	String (6..50)	Dieses Datenfeld enthält die vom Nutzer eingegebene Passwort-Wiederholung, die identisch zu "password" sein soll. Die Wiederholung soll Tippfehler bei der Eingabe erkennen.

Tabelle 3.101 Parameter des Profils "Aufrufparameter für Passwortänderung" (passwordUpdateParameters)

3.22.37 Proxy-Kommunikationsprofil

Die transparente Datenkommunikation zwischen CLS und EMT erfordert die Konfiguration sogenannter *Proxy-Kommunikationsprofile* im SMGW. Mit einem Proxy-Kommunikationsprofil werden die Kommunikationsberechtigungen mit dem SMGW und die zulässigen Datenflüsse zwischen einem CLS und einem EMT konfiguriert. Es können mehrere Proxy-Kommunikationsprofile je CLS/EMT definiert werden.

Parameter	Datentyp	Beschreibung
Profil-ID (profileId)	String (name)	Dieses Datenfeld identifiziert das Proxy-Kommunikationsprofil unter allen Proxy-Kommunikationsprofilen an den Schnittstellen des SMGW eindeutig. Dieses Datenfeld dient als Ressourcen-Identifikation.
WAN-Kommunikationsreferenz (wanPeerRef)	String (name)	Dieser Parameter enthält eine Referenz auf das für die Kommunikation mit dem aktiven EMT zu verwendende WAN-Kommunikationsprofil vom Typ WKS.TLSPROXY (profileId)
HAN-Kommunikationsreferenz (hanPeerRef)	String (name)	Dieser Parameter enthält eine Referenz auf das für die Kommunikation mit dem CLS zu verwendende HAN-Kommunikationsprofil vom Typ HKS.TLSPROXY.* (profileId)
Parameter der Proxy-Funktion		
Lokaler Server-Name (localServerName) (optional)	String (name)	Sofern dieser Parameter leer oder nicht vorhanden ist, wird die wanPeerRef eingesetzt. Die Bedeutung des Feldes unterscheidet sich nach Inhalt des Datenfeldes "hks". Für TLSPROXY.SRV: Der "localServerName" wird case-insensitiv mit dem vom CLS im Verbindungsaufbau gesendeten Server-Name Indication "dnsName" verglichen. Für TLSPROXY.CLI: Der "localServerName" wird im TLS-Verbindungsaufbau als Server-Name Indication an das CLS übermittelt. Für TLSPROXY.SOCKS mit Adresstyp "Domainname": Der "localServerName" wird case-insensitiv mit dem vom CLS im SOCKS-CONNECT gesendeten Domain-Namen verglichen. Hinweis: Für TLSPROXY.SOCKS mit Adresstyp "IPv4" ist "localServerName" nicht vorhanden, da die IP-Adresse mit der IP-Adresse des über "wanPeerRef" referenzierten WAN-Kommunikationsprofils verglichen wird.
CLS-Proxy Priorität (channelPrio) (optional)	Integer (0..255)	Sofern der optionale Parameter nicht vorhanden ist, beschreibt der GWH nach welcher Bedingung eine TLS-Proxy-Verbindung in Engpasssituationen abgebaut wird. (Standardwert: 0) Dieser Parameter bietet die Möglichkeit zu definieren, welches Proxy-Kommunikationsprofil und damit welche Proxy-Verbindung Vorrang bekommt bei Konfliktsituationen zwischen mehreren Proxy-Verbindungen. Höherere Werte entsprechen höherer Priorität.

Parameter	Datentyp	Beschreibung
Proxy-Start-Ereignis (triggerTime) (optional)	Tupel	Sofern dieser optionale Parameter angegeben ist, wird der Proxy-Kanal zeitgesteuert vom SMGW aufgebaut. Dieser Parameter legt den (wiederkehrenden) Zeitpunkt fest, an dem das SMGW Proxy-Verbindungen zu CLS und aktivem EMT aufbaut. Der Parameter setzt Kommunikationsszenarien mit abgehender TLS-Verbindung voraus.
Tag (day) (optional)	Integer (1..31)	Sofern dieser optionale Parameter nicht angegeben ist, wird die Verbindung täglich initiiert. Dieser Parameter definiert den Tag (des Monats) an dem eine Verbindung vom SMGW iniitiert werden soll.
Stunde (hour) (optional)	Integer (0..23)	Sofern dieser optionale Parameter nicht angegeben ist, wird die Verbindung stündlich initiiert. Dieser Parameter definiert die Stunde (des Tages) an der eine Verbindung vom SMGW initiiert werden soll.
Minute (min) (optional)	Integer (0..59)	Sofern dieser optionale Parameter nicht angegeben ist, wird die Verbindung minütlich initiiert. Dieser Parameter definiert die Minute (der Stunde) an der eine Verbindung vom SMGW initiiert werden soll.
Proxy-Kanal-Status (channelStatus) (optional)	Boolean	Darf beim anlegen und aktualisieren des Profils nicht vorhanden sein Zustand des Proxy-Kanals. Sofern sowohl die Verbindung zum CLS als auch zum EMT aufgebaut ist, wird dieses Datenfeld true, anderenfalls ist es false.
Erweiterungen (extensions) (optional)	Any	Ist dieses optionale Datenfeld vorhanden, kann der GWA herstellerspezifische Erweiterungen zur Verbindungsherstellung übergeben, die im SMGW persistiert werden. Für die herstellerspezifischen Erweiterungen ist das Default-Verhalten des SMGW zu beschreiben, sofern dieses Datenfeld nicht vorhanden ist. Damit soll gewährleistet werden, dass das SMGW auch mit GWA-Systemen interoperabel ist, die die Erweiterungen nicht unterstützen. Siehe auch ▸ICS.HAN.ProxyKommunikationsprofile.10.

Tabelle 3.102 Parameter des Profils "Proxy-Kommunikationsprofil" (proxyCommunicationProfile)

Proxy-Kommunikationsprofile werden als Ressource an den Schnittstellen über die eindeutige Profil-ID referenziert.

Proxy-Kommunikationsprofile werden über die eindeutige Profil-ID referenziert.

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

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



ICS.HAN.ProxyKommunikationsprofile.10

Der GWH **MUSS** im ICS erklären, ob das SMGW das Datenfeld Erweiterungen im Proxy-Kommunikationsprofil verarbeitet. In diesem Fall muss der GWH das Verhalten des SMGW beschreiben, sofern Datenfelder mit herstellerspezifischen Erweiterungen des SMGW nicht vorhanden sind.

3.22.38 Status einer Proxy-Verbindung

Diese Datenstruktur beschreibt die Mindestanforderungen an die Statusdaten einer Proxy-Kommunikationsverbindung.

Datenfeld	Datentyp	Beschreibung
Profil-ID des zugeordneten Proxy-Kommunikationsprofiles (profileRefId)	String (name)	Dieses Datenfeld identifiziert das Proxy-Kommunikationsprofil, dem diese Statusinformationen zugeordnet sind. Dieses Datenfeld dient als Ressourcen-Identifikation.
Proxy-Kanal Zustand (established)	Boolean	Zustand des Proxy-Kommunikationskanales. true: Lokale- und WAN-Verbindung sind TLS-authentifiziert aufgebaut.
Lokaler Verbindungszustand (localConnectionState) (optional)	Enumeration • IDLE • CONNECTING • CONNECTED • ERROR_NETWORK • ERROR_CONNECTING • ERROR_AUTH	Dieses Datenfeld kann entfallen, wenn der Proxy-Kanal vollständig aufgebaut ist. (Standardwert: CONNECTED) Dieses Datenfeld beschreibt den Zustand der lokalen Verbindung zum CLS. Die Wertebelegungen haben folgende Bedeutung: • IDLE: Ruhezustand • CONNECTING: Verbindungsaufbau • CONNECTED: Verbunden • ERROR_NETWORK: Netzwerkzugangsfehler • ERROR_CONNECTING: Verbindungsfehler • ERROR_AUTH: TLS-Authentifizierungsfehler
WAN Verbindungszustand (wanConnectionState) (optional)	Enumeration • IDLE • CONNECTING • CONNECTED • ERROR_NETWORK • ERROR_CONNECTING • ERROR_AUTH	Dieses Datenfeld kann entfallen, wenn der Proxy-Kanal vollständig aufgebaut ist. (Standardwert: CONNECTED) Dieses Datenfeld beschreibt den Zustand der Verbindung zum EMT. Die Wertebelegungen haben folgende Bedeutung: • IDLE: Ruhezustand • CONNECTING: Verbindungsaufbau • CONNECTED: Verbunden • ERROR_NETWORK: Netzwerkzugangsfehler • ERROR_CONNECTING: Verbindungsfehler • ERROR_AUTH: TLS-Authentifizierungsfehler
Erweiterungen (extensions) (optional)	Any	Ist dieser optionale Parameter vorhanden, kann der GWH herstellerspezifische Erweiterungen zum Zustand des Proxykanals ausgeben. Dieses Datenfeld enthält herstellerspezifische Statusinformationen zum Zustand des Proxykanals.

Tabelle 3.103 Datenfelder des Datenobjekts "Status einer Proxy-Verbindung" (proxyStatus)

3.22.39 RootCA-Zertifikatssatz

Die folgende Datenstruktur enthält die Aufrufparameter für den Import eines neuen Root-CA-Zertifikates.

Parameter	Datentyp	Beschreibung
RootCA-Zertifikat (rootCert)	String (hexString)	Neues Wurzelzertifikat der SM-PKI (siehe [SM-PKI-CP]) zur Validierung Zertifikatskette. Das Zertifikat entspricht dem Zertifikatsprofil C(Root) gemäß [TR-03109-4].
RootCA-Link-Zertifikat (linkCert) (optional)	String (hexString)	Sofern dieses optionale Datenfeld nicht vorhanden ist, kann das SMGW neue RootCA-Zertifikat nicht (über das Link-Zertifikat) mit dem zeitlich vorhergehenden RootCA-Zertifikat validieren. Zur Verwendung des Link-Zertifikat siehe [TR-03109-4] Kap 3.3.2.2. Es ist vom zeitlich vorhergehenden RootCA-Zertifikat signiert.

Parameter	Datentyp	Beschreibung
Root-Schlüssel CV-Zertifikat (rootKeyCv-Cert)	String (hexString)	Enthält eine CV-Datenstruktur (siehe [TR-03109-2]) zum Import des RootCA-Public-Keys in das Sicherheitsmodul des SMGW.

Tabelle 3.104 Parameter des Profils "RootCA-Zertifikatssatz" (rootCaCertificateSet)

3.22.40 Sicherheitsmodulzustand

Die folgende Tabelle enthält eine Datenstruktur zur Übermittlung des Zustandes des Sicherheitsmoduls.

Datenfeld	Datentyp	Beschreibung
Schlüsselobjekte (keyObjects)	Array [0..99] von Tupel	Liste der GWA-Schlüsselobjekte
Name des Schlüsselobjekts (keyObject) (optional)	Enumeration • GWA_TLS_PUB_1 • GWA_SIG_PUB_1 • GWA_ENC_PUB_1 • GWA_AUT_PUB_1 • GWA_TLS_PUB_2 • GWA_SIG_PUB_2 • GWA_ENC_PUB_2 • GWA_AUT_PUB_2 • ROOTCA_PUB_1 • ROOTCA_PUB_2 • ROOTCA_PUB_3 • ROOTCA_PUB_4 • ROOTCA_PUB_5 • ROOTCA_PUB_6 • ROOTCA_PUB_7 • ROOTCA_PUB_8 • ROOTCA_PUB_9 • ROOTCA_PUB_10	Ist dieses optionale Datenfeld nicht vorhanden, kann das SMGW keine Zuordnung zwischen Schlüsseltyp und Schlüsselobjekt bereitstellen. Beschreibt die Verwendung des Schlüssels. Das Sicherheitsmodul besitzt zwei Schlüsselbänke für GWA-Schlüssel.: GWA_TLS/SIG/ENC/AUT/_PUB_1/2, ROOTCA_PUB_1..10
Schlüsselreferenz-ID (keyId)	String (hexString)	Die Schlüsselreferenz im Sicherheitsmodul
PublicKey (key)	String (hexString)	Der im Schlüsselobjekte gespeicherte Public Key
RootCA-Zertifikate (rootCaCerts)	Array [0..10] von Tupel	Liste der im Sicherheitsmodul gespeicherten RootCA-Zertifikate
Zertifikat (cert)	String (hexString)	Das im Sicherheitsmodul gespeicherte Zertifikat
GWA am Sicherheitsmodul authentifiziert (gwaAuthState) (optional)	Boolean	Ist dieses optionale Datenfeld nicht vorhanden, kann keine Aussage über die Authentifizierung am Sicherheitsmodul gemacht werden. true: Der GWA ist am Sicherheitsmodul authentifiziert

Datenfeld	Datentyp	Beschreibung
Erweiterungen (extensions) (optional)	Any	Ist dieses Datenfeld vorhanden, können herstellerspezifische Erweiterungen verwendet werden. Das Datenfeld dient der Ausgabe weiterer Informationen.

Tabelle 3.105 Datenfelder des Datenobjekts "Zustand des Sicherheitsmoduls" (secmodKeyState)

Das SMGW **KANN** weitere Datenfelder für den Sicherheitsmodulzustand unterstützen. [REQ.FAKAT.SmgwCertMgmt.60]



ICS.FAKAT.SmgwCertMgmt.40

Der GWH **MUSS** im ICS erklären, ob das SMGW das Datenfeld Erweiterungen im Sicherheitsmodulzustand ausgibt. In diesem Fall muss der GWH die Bedeutung beschreiben.

3.22.41 Parameter für den Aufruf von Selbsttests

Diese Datenstruktur beschreibt die Mindestanforderungen an Aufrufparameter für Selbsttests.

Die Parameter werden nicht persistiert.

Parameter	Datentyp	Beschreibung
Zweck des Selbsttests (purpose)	Enumeration • Befundprüfung (NOTIFIED_BODY_REQUEST) • Nach Update (AFTER_UPDATE)	Dieses Datenfeld enthält den Zweck bzw. Auslöser des Selbsttestes für eine Protokollierung in den Logs.

Tabelle 3.106 Parameter des Profils "Selbsttest Parameter" (selftestParameters)

3.22.42 SMGW-Zertifikatssatz

Die folgende Datenstruktur enthält die Aufrufparameter für den Import der SM-PKI-Zertifikate des SMGW.

Parameter	Datentyp	Beschreibung
TLS-Zertifikat (tlsCert)	String (hexString)	GW_WAN_TLS_CRT gemäß [TR-03109-4] und [SM-PKI-CP] Anhang A mit Funktion "smgw". Wird für die TLS-Authentifizierung verwendet.
Signaturzertifikat (sigCert)	String (hexString)	GW_WAN_SIG_CRT gemäß [TR-03109-4] mit SubjectDN und IssuerDN identisch zum TLS-Zertifikat. Wird zur Validierung von Inhaltsdaten verwendet.
Verschlüsselungszertifikat (encCert)	String (hexString)	GW_WAN_ENC_CRT gemäß [TR-03109-4] mit SubjectDN und IssuerDN identisch zum TLS-Zertifikat. Wird für Inhaltsdatenverschlüsselung verwendet.
SubCA-Zertifikat zu den Zertifikaten des SMGW (caCert) (optional)	String (hexString)	Sofern dieser optionale Parameter nicht vorhanden ist, kann das SMGW dem Kommunikationspartner im TLS-Handshake oder CMS-signierter Nachricht kein Ausstellerzertifikat zum SMGW-SM-PKI Endnutzer-Zertifikat bereitstellen. SUBCA_WAN_SIG_CRT gemäß [TR-03109-4] mit SubjectDN identisch zum IssuerDN des TLS-Zertifikates. Das Signaturzertifikat der SubCA, welche die Zertifikate innerhalb dieses Profils ausgestellt hat. Dieses Zertifikat kann dem Kommunikationspartner des SMGW beim TLS-Handshake bereitgestellt werden. Es ist nicht zwingend erforderlich.

Tabelle 3.107 Parameter des Profils "SMGW-Zertifikatssatz" (smgwCertificateSet)

3.22.43 Tageswert und Tageswertliste (TWL)

Die Tageswerte werden einmal täglich je Messeinrichtung erfasst und enthalten historische Verbrauchsinformationen.

Die TWL dient der Erfüllung des Rechtsrahmens (§ 61 und 62 MsbG) bei gleichzeitiger Einsparung von Speicherplatz im SMGW über den Vorhaltezeitraum. Da an die Tageswerte nicht die höheren Anforderungen an zeitliche Fehlergrenzen zur gesetzlichen Zeit gestellt werden, aber längere Vorhaltefristen gelten, wird dem Implementierer mit dieser Datenstruktur die Möglichkeit gegeben beim Export die Werte aus der ▸RWL zu erzeugen oder separate Ringspeicher für die ▸TWL vorzusehen.

3.22.43.1 TWL

Datenfeld	Datentyp	Beschreibung
Messgeräteidentifikation (meterId)	String (huid)	Dieses Datenfeld enthält die herstellerübergreifende Identifikationsnummer der Messeinrichtung, die Ursprung der Messwerte in dieser TWL ist.
Intervall (interval)	Enumeration • DAILY	Dieses Datenfeld enthält das in der Tageswertliste verwendete Intervall, in dem Tageswerte aufgenommen werden. Die Wertebelegungen haben folgende Bedeutung: • DAILY: Es wird genau ein Wert pro Tag aufgenommen.
Spalten (columns)	Array [0..n] von Tupel	Spaltenüberschriften für die "Messwerte (values)" der enthaltenen "Tageswerte (meterReadings)". Siehe auch ▸Abschnitt 3.22.3.
OBIS-Kennzahl (obis)	String (obis)	Dieses Datenfeld identifiziert das Medium, die Messgröße und die Messart des zugehörigen Messwerts.
Einheit (unit)	String (0..5)	Dieses Datenfeld beschreibt die Einheit des zugehörigen Messwerts. Der zu verwendende Wert ist abhängig von der oben angegebenen OBIS-Kennzahl. Siehe auch ▸Abschnitt 2.5.2.
Tageswerte (meterReadings)	Array [0..n] von Tupel	Dieses Datenfeld enthält einzelne Tageswerte.
Hierunter befinden sich die einzelnen Tageswerte. Folgende Elemente sind an dieser Stelle möglich: • DailyMeterReading (definiert in ▸Tabelle 3.109)		

Tabelle 3.108 Datenfelder des Datenobjekts "Tageswertliste (TWL)" (dailyMeterReadingList)

3.22.43.2 Tageswert

Datenfeld	Datentyp	Beschreibung
Bezugszeitpunkt des Tageswerts (refTs)	String (dateTime)	Dieses Datenfeld enthält den Sollzeitpunkt, zu dem der Tageswert zugeordnet ist.
Zeitstempel des Messwerts (ts)	String (dateTime)	Dieses Datenfeld wird aus der Messwertzulieferung übernommen.
Zeitstempel aus Messeinrichtung (measurementTs) (optional)	String (dateTime)	Dieses Datenfeld ist nur vorhanden, wenn die Messeinrichtung einen Zeitstempel für die Messung bereitstellt. Dieses Datenfeld wird aus der Messwertzulieferung übernommen.
Messwerte (values)	Array [0..n] von Tupel	Dieses Datenfeld enthält eine Menge von Messwerten. Ist der Gesamtstatus "Fehlender Wert", dann enthält der Eintrag keinen neuen Messwert. Weitere Informationen zum Messwert werden über das Datenfeld "Spalten" der übergeordneten TWL festgelegt.
Messwert (value)	Number	Dieses Datenfeld enthält den Messwert
Kombiniertes Statuswort (combinedStatus)	Tupel	Dieses Datenfeld enthält Statusinformationen.

Datenfeld	Datentyp	Beschreibung
Hierin enthalten sind die Gerätestatusinformationen der Messeinrichtung und des SMGW. Folgende Elemente sind an dieser Stelle möglich: • CombinedStatus (definiert in ▸Tabelle 3.74)		

Tabelle 3.109 Datenfelder des Datenobjekts "Tageswert" (dailyMeterReading)

3.22.44 Tarifzustand

Der Tarifzustand enthält für Tarifanwendungsfälle die abgeleitete Werte bilden, den aktuellen Zustand des Verarbeitungsprogrammes. Dazu gehört der aktuelle Stand der abgeleiteten Werte, die Tarifstufe und die zur Verarbeitung verwendete aktuelle Zeit.

Datenfeld	Datentyp	Beschreibung
Aktuelle Zeit (currentTime)	String (dateTime)	Aktuelle Systemzeit zum Zeitpunkt der Erstellung der Datenstruktur (UTC mit lokalem Zeitoffset).
Kombiniertes Statuswort (combinedStatus)	Tupel	Dieses Datenfeld enthält Statusinformationen.
Hierin enthalten sind die Gerätestatusinformationen der Messeinrichtung und des SMGW zum zuletzt registrierten Messwert. Folgende Elemente sind an dieser Stelle möglich: • CombinedStatus (definiert in ▸Tabelle 3.74)		
Messwerte (values)	Array [0..n] von Tupel	Der Inhalt der Register zum Zeitpunkt "currentTime" Die Anzahl "n" der Register und die OBIS-IDs sind durch die Versandmesswerte-Konfiguration des Auswertungsprofiles und "tafType" bestimmt
OBIS-ID (obis)	String (obis)	OBIS-ID des Messwertes
Messwert (value)	Number	Wert des Messwertes
Einheit (unit)	String (0..5)	Einheit des Messwertes (z.B kWh)
Aktuelles Zählregister (currentRegister) (optional)	String (obis)	Dieses Datenfeld ist nur vorhanden, wenn die Datenstruktur einem Auswertungsprofil mit Tarifstufen zugeordnet ist (TAF2) Enthält die Identifikation des aktuell aktiven Zählregisters. Die OBIS Value-Group E entspricht der Tarifstufe (1-63).
Preisbestandteile (priceComponents) (optional)	Tupel	Dieses Datenfeld ist nur vorhanden, wenn im zugeordneten Auswertungsprofil für die aktuelle Tarifstufe Preisbestandteile konfiguriert sind Dieser Parameter enthält einen oder mehrere Preisbestandteile für das aktuell aktive Zählregister.
Name des Preisbestandteil (name)	String (1..32)	Name des Preisbestandteils einschließlich Hinweis auf brutto bzw. netto.
Preis des Preisbestandteils (amount)	Number	Der aufgerufene Preis für den benannten Preisbestandteil in Cent.
Nächster Aktualisierungszeitpunkt (nextRefreshTime) (optional)	String (dateTime)	Dieses Datenfeld ist vorhanden, sofern ein Abrechnungsturnus (bei TAF2 und TAF8) im Auswertungsprofil angegeben ist Enthält den nächsten vorgesehenen Zeitpunkt, zu dem ein neuer abgeleiteter Wert gebildet wird. Aktuelle Registerwerte werden unabhängig vom Abrechnungsturnus gebildet und beeinflussen den hier enthaltenen Zeitpunkt nicht.

Datenfeld	Datentyp	Beschreibung
Zählzeitdefinition (timeOfUseDefinition) (optional)	Array [1..4] von Tupel	Dieses Datenfeld ist nur für TAF2 vorhanden. Dieses Datenfeld enthält die verwendete Zählzeitdefinition aus dem Auswertungsprofil. Enthalten ist dabei die aktuell verwendete Definition (letzter Zeitpunkt in der Vergangenheit gemäß Systemzeit) und die drei nachfolgenden Definitionen in der Zukunft (sofern vorhanden).
OBIS-Kennzahl des zu verwendenden Registers (obis)	String (obis)	Dieses Datenfeld entspricht dem Parameter des Auswertungsprofils und legt fest, in welches Register Energiemengen ab dem angegebenen Zeitpunkt kumuliert werden sollen.
Zeitpunkt (time)	String (dateTime)	Dieses Datenfeld entspricht dem Parameter des Auswertungsprofils und definiert den Zeitpunkt, zu dem das per OBIS-Kennzahl definierte Register aktiv werden soll und damit als Zielregister für die Kumulierung von Energiemengen verwendet wird.

Tabelle 3.110 Datenfelder des Datenobjekts "Tarifzustand" (tariffState)

3.22.45 WAN-Schnittstellenkonfigurationsprofil

WAN-Schnittstellenkonfigurationsprofile legen die Parameter für die Konfiguration der WAN-Schnittstelle des SMGW fest.

Parameter	Datentyp	Beschreibung
Profil-ID (profileId)	String (name)	Der im SMGW eindeutige Bezeichner des WAN-Schnittstellenkonfigurationsprofils.
Schnittstellenbezeichnung (ifName) (optional)	String (name)	Fehlt dieser Parameter, wird der Default-Wert verwendet. (Standardwert: WAN1) Im SMGW eindeutige Bezeichnung der physischen WAN-Schnittstelle. Beginnt mit "WAN"
Host-IPv4 Adresskonfiguration (hostIpv4Addr) (optional)	Tupel	Fehlt dieser optionale Parameter, werden im WAN-Host-IPv4-Adressen vom WAN-Zugangsnetzwerk-Zugangspunkt bezogen. Legt fest, wie das SMGW die IPv4-Adresse(n) der WAN-Schnittstelle bestimmt.
Modus (mode) (optional)	Enumeration • AccessPoint • DHCP • Static	Fehlt dieser Parameter, wird der Default-Wert verwendet. (Standardwert: AccessPoint) Legt die Betriebsart fest, wie das SMGW die IP-Adresse(n) der WAN-Schnittstelle bestimmt. Die Wertebelegungen haben folgende Bedeutung: • AccessPoint: Wird "AccessPoint" angegeben, werden abhängig vom Link-Layer Protokoll zum Zugangsnetz, Protokolle wie PPP/IPCP, DHCPv4 zum Bezug der IPv4-Adressen verwendet. • DHCP: Wird "DHCP" angegeben, wird die IPv4 Adresse im WAN mittels DHCP bezogen. • Static: Wird "Static" angegeben, wird die im Datenfeld ip4Addr angegebene Adresse statisch verwendet.
IPv4-Adresse (ipv4Addr) (optional)	String (ipv4)	Dieser Parameter wird für den Adressmode "Static" benötigt. Legt die IPv4-Adresse der Schnittstelle als Dotted-Decimal-Notation fest.
IPv4-Subnetzmaske (ipv4Mask) (optional)	String (ipv4)	Dieser Parameter wird für den Adressmode "Static" benötigt. Wird er nicht angegeben wird eine Punkt-zu-Punkt Subnetzmaske 255.255.255.255 verwendet. Legt die IPv4-Subnetzmaske der Schnittstelle als Dotted-Decimal-Notation fest.

Parameter	Datentyp	Beschreibung
IPv4-Gateway (ipv4gateway) (optional)	String (ipv4)	Dieser Parameter wird für den Adressmode "Static" benötigt. Wird er nicht angegeben, wird kein IP-Routing an der WAN-Schnittstelle verwendet. Legt die IPv4-Adresse des Routers im WAN-Zugangsnetzwerk fest.
Host-IPv6 Adresskonfiguration (hostIpv6Addr) (optional)	Tupel	Fehlt dieser Optionale Parameter, werden routbare WAN-Host-IPv6-Adressen mit Unterstützung des WAN-Zugangsnetzwerk-Zugangspunktes bestimmt. Legt fest, wie das SMGW die IPv6-Adresse(n) der WAN-Schnittstelle bestimmt.
Modus (mode) (optional)	Enumeration • AccessPoint	Fehlt dieser Parameter, wird der Default-Wert verwendet. (Standardwert: AccessPoint) Legt die Betriebsart fest, wie das SMGW die IPv6-Adresse(n) der WAN-Schnittstelle bestimmt. Die Wertebelegungen haben folgende Bedeutung: • AccessPoint: Wird "AccessPoint" angegeben, werden abhängig vom Link-Layer Protokoll zum Zugangsnetz, Protokolle wie PPP/IPV6CP oder SLAAC zum Bezug des Interface-Identifiers für routbare IPv6-Adressen verwendet.
Erweiterungen (extensions) (optional)	Any	Ist dieser optionale Parameter vorhanden, kann der GWA herstellerspezifische Erweiterungen zur Verbindungsherstellung übergeben, die im SMGW persistiert werden. Für die herstellerspezifischen Erweiterungen ist das Default-Verhalten des SMGW zu beschreiben, sofern dieser Parameter nicht vorhanden ist. Damit soll gewährleistet werden, dass das SMGW auch mit GWA-Systemen interoperabel ist, die die Erweiterungen nicht unterstützen.

Tabelle 3.111 Parameter des Profils "WAN-Schnittstellenkonfigurationsprofil" (wanIfProfile)

Das SMGW kann im Datenfeld "Erweiterungen" weitere Parameter für Schnittstellenkonfigurationsprofile unterstützen.

Implementation Conformance Statements



ICS.WAN.IfProfile.10

Der GWH **MUSS** im ICS erklären, ob das SMGW das Datenfeld Erweiterungen im WAN-Schnittstellenkonfigurationsprofil verarbeitet. In diesem Fall muss der GWH das Verhalten des SMGW beschreiben, sofern Datenfelder mit herstellerspezifischen Erweiterungen des SMGW nicht vorhanden sind.

3.22.46 WAN-Kommunikationsprofile

WAN-Kommunikationsprofile legen die Parameter für die Kommunikation mit einem EMT oder GWA im WAN fest.

Ein WAN-Kommunikationsprofil mit WKS "INFO-REPORT" wird in diesem Dokument auch als EMT-Kommunikationsprofil bezeichnet. Ein WAN-Kommunikationsprofil mit WKS "MANAGEMENT", "ADMIN-SERVICE", "DOWNLOAD", "NTP-TLS" wird in diesem Dokument auch als GWA-Kommunikationsprofil bezeichnet.

Parameter	Datentyp	Beschreibung
Profil-ID (profileId)	String (name)	Dieses Datenfeld identifiziert das WAN-Kommunikationsprofil unter allen WAN-Kommunikationsprofilen an den Schnittstellen des SMGW eindeutig. Dieses Datenfeld dient als Ressourcen-Identifikation.

Parameter	Datentyp	Beschreibung
WAN-Kommunikationsszenario (wks)	Enumeration • MANAGEMENT • ADMIN-SERVICE • NTP-TLS • DOWNLOAD • INFO-REPORT • TLSPROXY	Legt das Kommunikationsszenario fest. Einige der folgenden Datenfelder sind abhängig vom Kommunikationsszenario vorhanden.
Zertifikate des Kommunikationspartners (peerCerts) (optional)	Tupel	Sofern dieser optionale Parameter nicht vorhanden ist, werden bei einem Update des Kommunikationsprofils die vorhandenen Zertifikate nicht geändert. Identifiziert den Kommunikationspartner, dem dieses Kommunikationsprofil zugeordnet ist. Das TLS-Zertifikat wird für die TLS-Authentifizierung des Kommunikationspartners verwendet. Die Rolle des Kommunikationspartners ist im Subject CommonName-Attribut des Zertifikates angegeben und muss zum Kommunikationsszenario passen. Dieser Parameter muss beim Anlegen des WAN-Kommunikationsprofils vorhanden sein.
TLS-Zertifikat (tlsCert)	String (hexString)	CTls(ENu) gemäß [TR-03109-4] und [SM-PKI-CP] Anhang A mit Funktion "emt" oder "gwa". Das Zertifikat wird für die TLS-Authentifizierung verwendet (EMT_WAN_TLS_CRT bzw. GWA_WAN_TLS_CRT).
Signaturzertifikat (sigCert)	String (hexString)	CSign(ENu) gemäß [TR-03109-4]. Das Zertifikat wird zur Validierung von Inhaltsdaten verwendet (EMT_WAN_SIG_CRT bzw. GWA_WAN_SIG_CRT).
Verschlüsselungszertifikat (encCert)	String (hexString)	CEnc(ENu) gemäß [TR-03109-4]. Das Zertifikat wird für Inhaltsdatenverschlüsselung verwendet (EMT_WAN_ENC_CRT bzw. GWA_WAN_ENC_CRT).
SubCA-Zertifikat zu den Zertifikaten des EMT (caCert) (optional)	String (hexString)	Wird dieses optionale Datenfeld nicht angegeben, dann muss das Sub-CA-Zertifikat für die Endnutzer-Zertifikate dieser Datenstruktur bereits im SMGW vorliegen oder im TLS-Handshake übermittelt werden. Der Inhalt des Datenfeldes ist ein Signaturzertifikat C(Sub-CA) gemäß [TR-03109-4] mit SubjectDN identisch zum IssuerDN des TLS-Zertifikates. Das SMGW verwendet dieses Zertifikat zur Kettenprüfung der Endnutzer-Zertifikate beim Import (SUBCA_WAN_SIG_CRT).
Nachrichtenformat (messageFormat) (optional)	Tupel	Sofern dieser optionale Parameter im WKS MANAGEMENT, ADMIN-SERVICE, INFO-REPORT nicht vorhanden ist, wird eine Nachricht mit den Defaults der folgenden Parameter (messageSigAlgo, messageEncryptionAlgo, messageCompressionAlgo) erzeugt. Für DOWNLOAD, NTP-TLS und TLSPROXY ist dieser Parameter nicht vorhanden. Dieses Datenfeld legt fest, welche Codierung und Verfahren für die Inhaltsdatensicherung beim Versand von Nachrichten an den Empfänger verwendet werden. Kryptografische Agilität erfordert die Vereinbarung kryptografischer Verfahren zwischen Absender und Empfänger.
Inhaltsdatensicherung entfällt (omitCms) (optional)	Boolean	Fehlt dieses optionale Datenfeld, wird die Inhaltsdatensicherung beim Versand von Nachrichten durchgeführt. (Standardwert: false) Bestimmt, ob die CMS-Inhaltsdatensicherung beim Versand von Nachrichten an den Empfänger entfällt.
Verbindungskonfiguration (outboundConnection)	Tupel	Definiert die Verbindungsparameter zum Aufbau einer abgehenden Verbindung.

Parameter	Datentyp	Beschreibung
Transportadresse(n) des Kommunikationspartners (addresses)	Array [1..n] von String (absolute-uri)	Legt mindestens eine Transportadresse fest, an denen der Kommunikationspartner Dienste für das SMGW anbietet und zu der eine TLS-Verbindung vom SMGW aufgebaut werden muss. Der String ist eine absolute URI gemäß [RFC3986]. Weitere Transportadressen könnten zur Verbesserung der Verfügbarkeit genutzt werden.
TLS-SNI (tlsSni) (optional)	String (name)	Wird dieses optionale Datenfeld nicht angegeben, dann wird der Name des WKS (z.B. "INFO-REPORT") als SNI gesendet Legt den beim Verbindungsaufbau in der Server-Name Indication zu verwendenden Namen fest.
WAN-Schnittstelle (ifName) (optional)	String (name)	Wird dieses optionale Datenfeld nicht angegeben, dann wird die vom GWH festgelegte primäre WAN-Schnittstelle verwendet (ICS). Legt die WAN-Schnittstelle des SMGW fest, über die Transportverbindung zur Adresse des Kommunikationspartners aufgebaut werden soll. Der Name beginnt mit "WAN".
Verbindung halten (keepOpen) (optional)	Boolean	Wird dieses optionale Datenfeld nicht angegeben, dann werden Verbindungen, bei denen das SMGW HTTP-Client ist, nach Empfang der Response vom SMGW geschlossen (Default: "false") und Verbindungen, bei denen das SMGW HTTP-Server ist, nach Versand der Response aufrechterhalten (Default: "true"). Legt fest, ob die TLS-Verbindung auch nach Abschluss der Request-Response-Transaktion aufrechterhalten werden soll. Das Verhalten des SMGW bei Kombinationen von keepOpen, idleTimeout und maxSessionDuration ist in den Anforderungen bei WAN-Verbindungen beschrieben. Siehe auch ▸Abschnitt 4.2.4. Siehe auch ▸ICS.WAN.Kommunikationsprofil.20.
Keepalive-Rate (keepAlive) (optional)	Integer (30..3600)	Wird dieses optionale Datenfeld nicht angegeben, dann werden keine TCP-Keepalives vom SMGW gesendet. Legt fest (in Sekunden) wie häufig das SMGW TCP-Keepalives sendet
Wiederholung fehlgeschlagener Verbindungsversuche (retryConfig) (optional)	Tupel	Ist dieser optionale Parameter nicht angegeben, gelten die Defaults der folgenden Datenfelder Bestimmt die Anzahl und Dauer zwischen den Versuchen zum Aufbau einer Transportverbindung.
Anzahl Runden (maxLoopCount) (optional)	Integer (1..65535)	Fehlt dieser optionale Parameter, wird eine Wiederholungsrunde durchgeführt (Standardwert: 1) Maximale Anzahl der Runden der Retries. Die maximale Gesamtzahl der Versuche ist maxLoopCount * maxRetryCount.
Protokollierung wenn die zweite oder eine weitere Runde gestartet wird (logLoopFailures) (optional)	Boolean	Fehlt dieser optionale Parameter, wird der Standardwert verwendet. (Standardwert: true) Ist der Wert "true", erfolgt ein Eintrag ins Logbuch, wenn die zweite oder eine weitere Runde gestartet wird.
Wartezeit zwischen zwei Runden (loopDelay) (optional)	Array [1..16] von Integer (0..86400)	Fehlt dieser optionale Parameter, wird der Standardwert verwendet. (Standardwert: 3600) Legt die Wartezeit zwischen zwei Runden fest (in Sekunden). Der erste Listeneintrag bestimmt die Wartezeit zwischen Runde 1 und Runde 2. Der zweite zwischen Runde 2 und Runde 3, usw. Die maximale Anzahl von Einträgen wird vom GWH im ICS beschrieben. Sind weniger Einträge als maxLoopCount vorhanden, wird der letzte Eintrag für die weiteren Runden verwendet.

Parameter	Datentyp	Beschreibung
Maximale Anzahl Wiederholversuche innerhalb einer Runde (maxRetryCount) (optional)	Integer (1..65535)	Fehlt dieser optionale Parameter wird der Standardwert verwendet. (Standardwert: 10) Maximale Anzahl der Retries innerhalb einer Runde.
Protokollierung wenn die zweite oder eine weitere Wiederholung gestartet wird (logRetryFailures) (optional)	Boolean	Fehlt dieser optionale Parameter, wird der Standardwert verwendet. (Standardwert: true) Ist der Wert "true", erfolgt ein Eintrag ins Logbuch, wenn die zweite oder eine weitere Wiederholung in einer Runde gestartet wird.
Wartezeit zwischen zwei Verbindungsaufbauversuchen (retryDelay) (optional)	Array [1..16] von Integer (0..86400)	Fehlt dieser optionale Parameter, wird der Standardwert verwendet. (Standardwert: 5) Legt die Wartezeit zwischen zwei Verbindungsaufbauversuchen fest (in Sekunden). Der erste Listeneintrag bestimmt die Wartezeit zwischen Versuch 1 und Versuch 2. Der zweite zwischen Versuch 2 und Versuch 3, usw. Die maximale Anzahl von Einträgen wird vom GWH im ICS beschrieben. Sind weniger Einträge als maxRetryCount vorhanden, wird der letzte Eintrag für die weiteren Runden verwendet.
Wartezeit im Leerlauf (idleTimeout) (optional)	Integer (0..999999)	Wird dieses optionale Datenfeld nicht angegeben, dann werden Verbindungen nach der Dauer gemäß Standardwert ohne Applikationsdatenaustausch abgebaut. (Standardwert: 300) Nach Ablauf der angegebenen Zeit (in Sekunden) ohne Applikationsdatenaustausch wird die TLS-Verbindung wieder abgebaut. Der Wert 0 deaktiviert den Abbau im Leerlauf. Das Verhalten des SMGW bei Kombinationen von keepOpen, idleTimeout und maxSessionDuration ist in den Anforderungen bei WAN-Verbindungen beschrieben. Siehe auch ▸Abschnitt 4.2.4.
Maximale Sitzungslänge (maxSessionDuration) (optional)	Integer (60..172800)	Wird dieses optionale Datenfeld nicht angegeben, dann wird die maximale Sitzungsdauer gemäß Vorgaben für die WAN-Schnittstelle gemäß [TR-03109-3] gewählt. Die maximale Zeit (in Sekunden), die eine TLS-Sitzung aufrechterhalten werden soll. Das Verhalten des SMGW bei Kombinationen von keepOpen, idleTimeout und maxSessionDuration ist in den Anforderungen bei WAN-Verbindungen beschrieben. Siehe auch ▸Abschnitt 4.2.4.
Service Timeout (serviceTimeout) (optional)	Integer (1..60)	Wird dieses optionale Datenfeld nicht angegeben, dann wird ein Standardwert angenommen. (Standardwert: 60) Die Dauer (in Sekunden), innerhalb der eine Antwort erwartet wird bzw. eine Antwort gesendet wird.

Parameter	Datentyp	Beschreibung
Erweiterungen (extensions) (optional)	Any	Ist dieser optionale Parameter vorhanden, kann der GWA herstellerspezifische Erweiterungen zur Verbindungsherstellung übergeben, die im SMGW persistiert werden. Für die herstellerspezifischen Erweiterungen ist das Default-Verhalten des SMGW zu beschreiben, sofern dieser Parameter nicht vorhanden ist. Damit soll gewährleistet werden, dass das SMGW auch mit GWA-Systemen interoperabel ist, die die Erweiterungen nicht unterstützen. Siehe auch ▸ICS.WAN.Kommunikationsprofil.10.

Tabelle 3.112 Parameter des Profils "WAN-Kommunikationsprofil" (wanCommunicationProfile)

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

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

Implementation Conformance Statements



ICS.WAN.Kommunikationsprofil.10

Der GWH **MUSS** im ICS erklären, ob das SMGW das Datenfeld Erweiterungen im WAN-Kommunikationsprofil verarbeitet. In diesem Fall muss der GWH das Verhalten des SMGW beschreiben, sofern Datenfelder mit herstellerspezifischen Erweiterungen des SMGW nicht vorhanden sind.



ICS.WAN.Kommunikationsprofil.20

Der GWH **MUSS** im ICS beschreiben, ob das SMGW den Parameter "Keepalive" aus ▸Tabelle 3.112 unterstützt.



ICS.WAN.Kommunikationsprofil.50

Der GWH **MUSS** im ICS beschreiben, ob das SMGW mehr als eine WAN-Schnittstelle besitzt. Im ICS wird beschrieben, welcher Wert im Datenfeld "wanIfc" die primäre Schnittstelle bezeichnet.

3.22.47 Zeitsynchronisationsstatus

Der Zeitsynchronisationsstatus beschreibt die Konfigurationsparameter, die das Verhalten des SMGW bei der Zeitsynchronisation mit dem Zeitserver des GWA beeinflussen. Der Systemuhr ist ein Datenobjekt Zeitsynchronisationsstatus zugeordnet.

Dieses Datenobjekt enthält nach der ersten erfolgreichen Zeitsynchronisation valide Werte.

Dieses Datenobjekt stellt die Qualitätsdaten für die Prüfung und Überwachung der Zeitführung des SMGW mit einheitlicher Semantik bereit.

Datenfeld	Datentyp	Beschreibung
Profil-ID (profileId)	String (name)	Dieses Datenfeld identifiziert das Zeitsynchronisationsstatusprofil unter allen Zeitsynchronisationsstatusprofilen an den Schnittstellen des SMGW eindeutig. Dieses Datenfeld dient als Ressourcen-Identifikation.
Geräte-ID (deviceId)	String (huid)	Dieser Parameter identifiziert das Gerät, dem das Zeitsynchronisationsstatusprofil zugeordnet ist.
Zeit valide (timeValid)	Boolean	Gibt an, ob die Systemzeit für Informationszwecke valide ist. Nach der letzten Synchronisierung mit der gesetzlichen Zeit ist weder die Gangreservedauer noch die Zeitsynchronisationsfehlerdauer überschritten worden.
Aktuelle valide Zeit (currentTime) (optional)	String (dateTime)	Ist die aktuelle Zeit nicht valide, ist dieses Datenfeld leer. Aktuelle Systemzeit (UTC mit lokalem Zeitoffset).

Datenfeld	Datentyp	Beschreibung
Letzter Zeitsynchronisationszeitpunkt (lastSyncTime) (optional)	String (dateTime)	Dieses optionale Datenfeld ist nicht vorhanden, wenn der letzte Synchronisationszeitpunkt nicht bekannt ist. Zeitpunkt der letzten erfolgreichen Zeitsynchronisation.
Letzte Zeitabweichung akzeptabel (lastDeviationOk)	Boolean	Gibt an, ob die bei der letzten Zeitsynchronisation festgestellte Abweichung der Systemzeit von der gesetzlichen Zeit innerhalb der "Maximalen Zeitabweichung" lag. Ist die letzte Zeitabweichung (z.B. wegen fehlender Zeitsynchronisation) nicht bekannt, ist dieses Datenfeld "false".
Zeitabweichung (deviation) (optional)	Integer (0..250000)	Dieses optionale Datenfeld ist nicht vorhanden, wenn die Abweichung nicht bekannt ist. Bei der letzten Zeitsynchronisation ermittelte Abweichung der Systemzeit vom Root-Zeitserver in Millisekunden (mit Vorzeichen) Die Berechnung erfolgt durch den NTP-Client basierend auf der halben Round-Trip-Zeit zum Root-Timeserver (root-delay) plus Abweichung (root-Dispersion).
Umlaufzeit (rtt) (optional)	Integer (0..10000)	Dieses optionale Datenfeld ist nicht vorhanden, wenn die RTT nicht bekannt ist. Bei der letzten Zeitsynchronisation ermittelte Round-Trip-Time (Delay) zwischen Absenden der NTP-Anforderung und Eintreffen der NTP-Antwort in Millisekunden.
Erweiterungen (extensions) (optional)	Any	Ist dieser optionale Parameter vorhanden, kann der GWH herstellerspezifische Erweiterungen zum Zustand der Zeitsynchronisation ausgeben. Dieses Datenfeld enthält herstellerspezifische Statusinformationen zum Zustand der Zeitsynchronisation.

Tabelle 3.113 Datenfelder des Datenobjekts "Zeitsynchronisationsstatus" (timeSyncStatus)

3.22.48 X.509-Zertifikat (Certificate)

Diese Datenstruktur enthält ein X.509-Zertifikat

Datenfeld / Parameter	Datentyp	Beschreibung
Zertifikat (cert)	String (hexString)	Dieses Datenfeld enthält ein X.509-Zertifikat.

Tabelle 3.114 Datenfelder / Parameter des Datenobjekts "X.509-Zertifikat" (certiciate)

4 Anforderungen an die Kommunikationsverbindungen und Protokolle des SMGW

4.1 Einleitung

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

Die Technische Richtlinie führt das Konzept eines Kommunikationsszenarios zur strukturierten Beschreibung von Anforderungen an die Kommunikationsverbindungen des SMGW ein. Ein Kommunikationsszenario benennt für die Protokollschichten gemäß OSI 7-Schichten Modell einer Schnittstelle die zu verwendenden Protokolle, Nachrichtenformate und die Rolle des SMGW gemäß Protokollschicht (z.B. Client/Server).

Die Kommunikationsszenarien referenzieren öffentlich zugängliche Schnittstellen-Protokoll-Spezifikationen, die idealerweise europäisch oder international im Konsens erarbeitet wurden. Anforderungen in den Kommunikationsszenarien konkretisieren, begrenzen oder erweitern die Universal-Anforderungen dieser Spezifikationen als Mindestanforderungen des BSI zur Interoperabilität des SMGW.

Detailspezifikationen zu dieser Technischen Richtlinie konkretisieren die Anforderungen der referenzierten Schnittstellen-Protokoll-Spezifikationen zur Verbesserung der Interoperabilität im intelligenten Messsystem, mit dem Ziel die Austauschbarkeit und Wechselprozesse weiter zu verbessern. Diese Detailspezifikationen werden regelmäßig überprüft und im Bedarfsfall nach Erfahrungen von Herstellern und Anwendern aktualisiert.

Die folgenden Abschnitte legen die Anforderungen an die Kommunikation über diese Schnittstellen im WAN (s. ▸Abschnitt 4.2), LMN (s. ▸Abschnitt 4.3) und HAN (s. ▸Abschnitt 4.4) fest.

Begriffsdefinition

In diesem Dokument wird zwischen einer *TLS-Verbindung* und einer *TLS-Session* unterschieden. Eine Verbindung impliziert bidirektionale Kommunikation zwischen SMGW und Kommunikationspartner. Die Lebenszeit einer *TLS-Session* (Sitzung) bezieht sich auf das TLS-Schlüsselmaterial und kann die Dauer einer *TLS-Verbindung* überschreiten. Mit Ende einer *TLS-Session* endet im TLS1.2 Protokoll auch die dazugehörige *TLS-Verbindung*. Im TLS1.3 Protokoll können die Sitzungsschlüssel - bei bestehender TLS-Verbindung - erneuert werden.

▸Abbildung 4.1 verdeutlicht die Zusammenhänge der Lebensdauer von TLS-Session, TLS-Verbindung und HTTP-Nachrichtenaustausch.

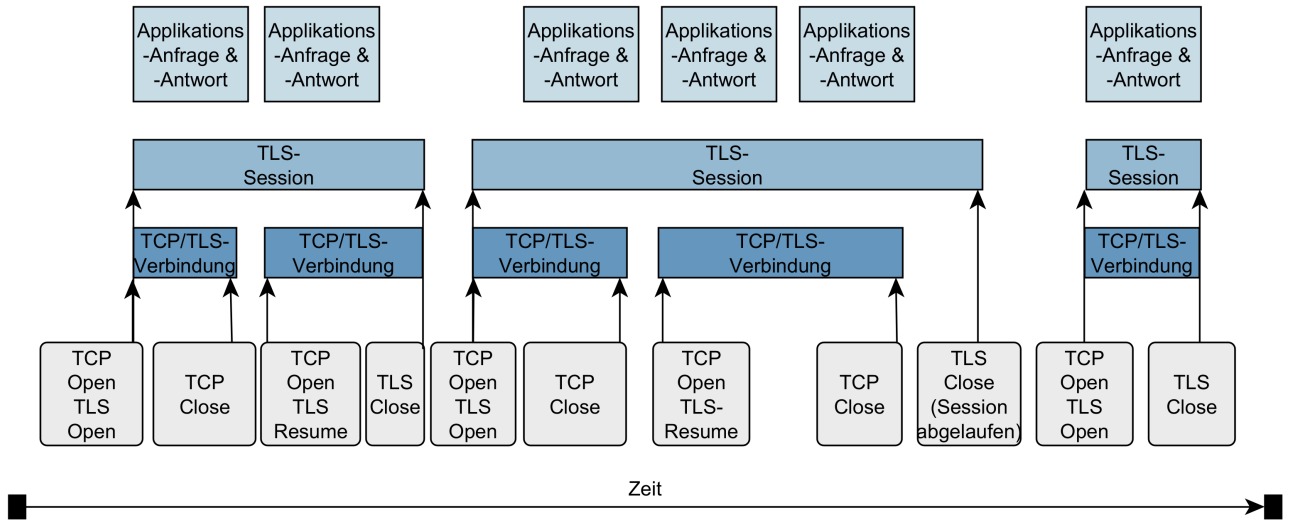


Abbildung 4.1. Lebensdauer von TLS-Session, TLS-Verbindung und HTTP-Nachrichtenaustausch

4.2 Kommunikation des SMGW im WAN

4.2.1 Einleitung

Das SMGW kommuniziert im WAN mit dem GWA, einem oder mehreren berechtigten EMT und einem oder mehreren berechtigten aktiven EMT. Anwendungsfälle, die eine WAN-Kommunikation erfordern, werden in ▸Kapitel 3 beschrieben. Zur Realisierung dieser Anwendungsfälle werden mehrere Kommunikationsszenarien herangezogen, die die Komposition der Protokolle bei der Kommunikation mit einem Kommunikationspartner beschreiben.

Das SMGW kommuniziert über physische Schnittstelle(n) zum WAN. Die WAN-Zugangstechnologie wird durch diese Technische Richtlinie nicht vorgegeben.

Die Parametrierung der Kommunikationsverbindungen wird durch den GWA über Kommunikationsprofile durchgeführt, die in ▸Abschnitt 3.22.46 beschrieben sind.

Das SMGW darf gemäß [PP-0073] keine TLS-Verbindungen akzeptieren, die von Teilnehmern aus dem WAN initiiert werden. Das SMGW kann jedoch über den Wake-Up Dienst (siehe ▸FA.InitiateManagementConnection) veranlasst werden, eine TLS-Verbindung zum GWA aufzubauen.

4.2.2 WAN-Kommunikationsszenarien

Die in ▸Kapitel 3 skizzierten Anwendungsfälle lassen sich an der WAN-Schnittstelle auf folgende Kommunikationsszenarien (gekennzeichnet mit dem Kürzel WKS) abbilden.

▸Tabelle 4.1 enthält für jedes WAN-Kommunikationsszenario eine Übersicht der Kommunikationsprotokoll-Rollen des SMGW und der technische Rolle des Kommunikationspartners.

- MANAGEMENT (Administration)

  Zugriff des GWA auf Services des SMGW, die das SMGW an seiner WAN-Schnittstelle dem GWA anbietet.

  Siehe ▸WKS.MANAGEMENT.

- ADMIN-SERVICE

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

  Siehe ▸WKS.ADMIN-SERVICE.

- INFO-REPORT

  Zugriff des SMGW auf Services des EMT oder GWA zum Versand von Daten durch das SMGW an den EMT.

  Siehe ▸WKS.INFO-REPORT.

- NTP-TLS

  Zeitsynchronisierung über einen vom GWA bereitgestellten NTP-Service.

  Siehe ▸WKS.NTP-TLS.

- TLSPROXY

  TLS-Kommunikationsverbindung vom SMGW zum aktiven EMT.

  Siehe ▸WKS.TLSPROXY.

- WAKEUP

  Anfordern einer MANAGEMENT-Verbindung durch den GWA.

  Siehe ▸WKS.WAKEUP.

- DOWNLOAD

  Laden einer Datei über einen Fileserver des GWA

  Siehe ▸WKS.DOWNLOAD.

Name des Szenarios	TLS-Server	Webservice-Server	Inhaltsdaten-Empfänger	Inhaltsdaten-Absender
MANAGEMENT	GWA	SMGW	GWA, SMGW[1]	GWA, SMGW
ADMIN-SERVICE	GWA	GWA	GWA	SMGW
INFO-REPORT	EMT, GWA	EMT, GWA	EMT	SMGW
NTP-TLS	GWA	-	-	-
TLSPROXY	aEMT	-	-	-
WAKEUP	-	-	SMGW	GWA
DOWNLOAD	GWA	GWA	SMGW	GWH

Tabelle 4.1 Kommunikationsszenarien an der WAN-Schnittstelle

4.2.3 WAN-Kommunikationsprotokolle

Die WAN-Kommunikationsszenarien sind aus einer Kombination von Kommunikationsprotokollen zusammengesetzt ("Protokollstapel"), die sich untergliedern in:

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

Die Kommunikation des SMGW über das WAN mit dem GWA bzw. mit EMT wird über die in ▸Abbildung 4.2 dargestellten Protokollstapel durchgeführt:

[1] Im Gegensatz zu den anderen Kommunikationsszenarien erlaubt WKS.MANAGEMENT sowohl das Einspielen als auch Auslesen von Informationen. Daher kann sowohl das SMGW als auch der GWA Inhaltsdaten-Empfänger sein.

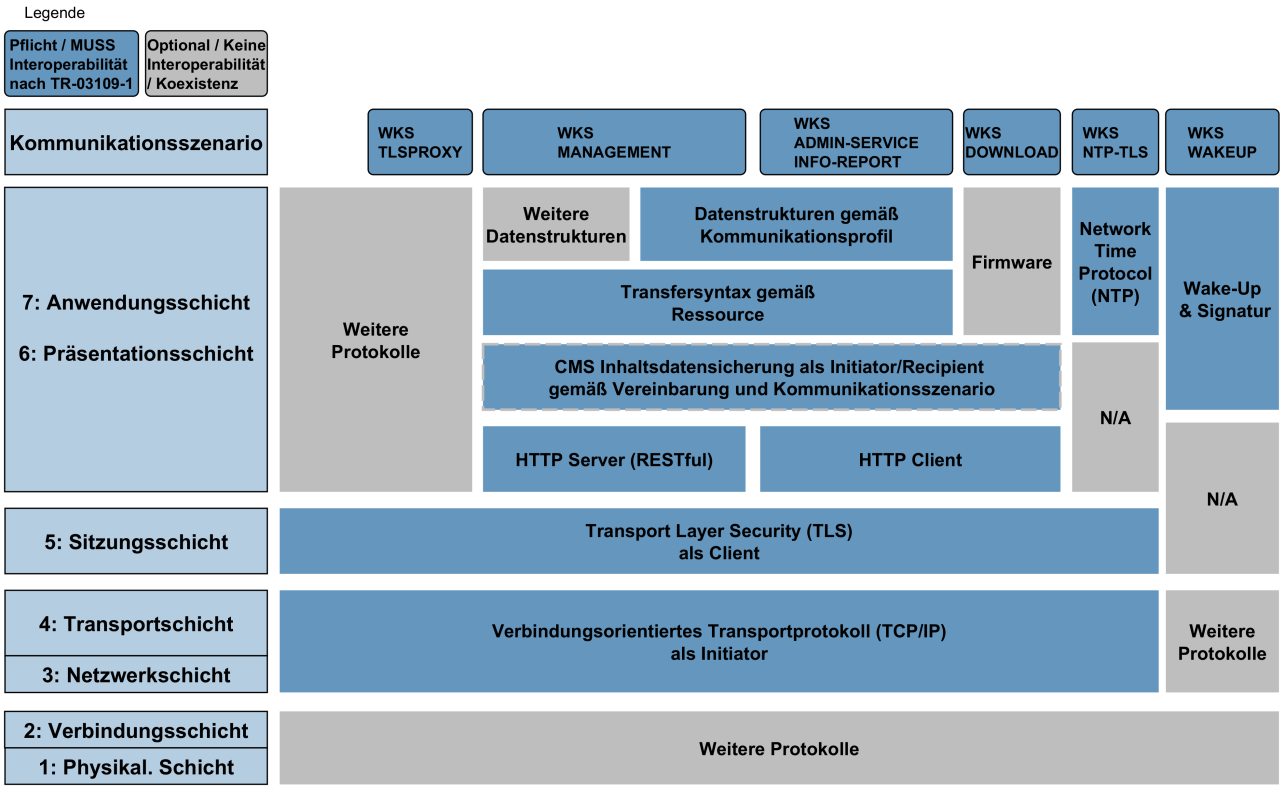


Abbildung 4.2. Protokollstapel für die WAN-Kommunikationsszenarien



Anmerkung

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

4.2.4 TLS-Verbindungen im WAN

Die folgenden Anforderungen gelten für die TLS-Verbindungen aller WAN-Kommunikationsprofile und Proxy-Kommunikationsprofile.

Verbindungsaufbau

- Innerhalb einer TLS-Verbindung des SMGW **MUSS** das Kommunikationsszenario ablaufen, das über ▸wks identifiziert ist. [REQ.WAN.Kommunikationsszenarien.30] Ein Wechsel des Kommunikationsszenarios innerhalb einer bestehenden TLS-Verbindung **DARF NICHT** vorgenommen werden. [REQ.WAN.Kommunikationsszenarien.40]
- Das SMGW **MUSS** in der Lage sein, Anwendungsdaten zu WAN-Kommunikationsszenarien über mindestens sechs TLS-Verbindungen gleichzeitig auszutauschen. [REQ.WAN.Kommunikationsszenarien.50] Das SMGW **MUSS** dabei mindestens drei TLSPROXY-Kanäle, einen MANAGEMENT-Kanal, mindestens eine GWA-Dienstverbindung (z.B. Zeitsynchronisation, ADMIN-SERVICE) und mindestens eine INFO-REPORT-Verbindung für Datenaustausch nutzen können. [REQ.WAN.Kommunikationsszenarien.51]
- Das SMGW **MUSS** gleichzeitig über zwei oder mehr TLS-Verbindungen mit dem GWA kommunizieren können (z.B. zum Management des Gateways und zur Fehlersignalisierung bzw. Alarmierung). [REQ.WAN.TlsSicherung.60]
- Falls die Systemzeit gemäß ▸REQ.WAF2.Zeitsynchronisation.50 nicht synchronisiert ist, **MUSS** das SMGW priorisiert gegenüber anderen WAN-Kommunikationsszenarien eine Zeitsynchronisation mit dem Zeitserver GWA durchführen. [REQ.WAN.TlsSicherung.80]
- Sofern der TCP-Verbindungsaufbau nicht innerhalb der in ▸outboundConnection.retryConfig.retryDelay definierten Zeit erfolgreich ist, **MUSS** das SMGW unmittelbar nach Ablauf dieser Zeit den nächsten Verbin-

dungsaufbau initiieren, solange ▸outboundConnection.retryConfig.maxRetryCount noch nicht erreicht ist. [REQ.WAN.Transport.50]

- Das SMGW **MUSS** den Aufbau der Verbindung endgültig als fehlgeschlagen betrachten, sofern die Zahl der maximalen Runden- und Wiederholversuchsanzahl gemäß ▸outboundConnection.retryConfig erreicht wurde. ▸ [FNN.2001.1] [REQ.WAN.Transport.51]
- Um eine Überlastung der GWA-Server nach Wiederkehr der Versorgungspannung oder der WAN-Kommunikation einer Vielzahl von SMGW zu vermeiden, **MUSS** das SMGW den ersten TLS-Verbindungsaufbau nach Neustart und Wiederkehr der WAN-Kommunikation so verzögern, dass Gleichzeitigkeitseffekte vermieden werden. [REQ.WAN.Transport.70] Dies kann beispielsweise durch eine zufällige Verzögerung innerhalb einer Zeitspanne von 60s erfolgen.
- Sofern ▸outboundConnection.keepOpen "true" und ▸outboundConnection.maxSessionDuration gleich "0" ist, **MUSS** das SMGW eine TLS-Verbindung nach dem Beenden (siehe ▸REQ.WAN.Transport.80) erneut aufgebaut. [REQ.WAN.Transport.81]
- Das SMGW **SOLL** beim TLS-Verbindungsaufbau den Inhalt des Datenfeldes ▸outboundConnection.tlsSni übermitteln. [REQ.WAN.Transport.90] Der TLS-Servername wird vom Kommunikationspartner case-insensitiv verarbeitet.

Authentifizierung

- Das SMGW **MUSS** den TLS-Handshake beenden, sofern das vom Kommunikationspartner empfangene Endnutzer-Zertifikat nicht aus der Smart Metering Public Key Infrastruktur gemäß [TR-03109-4] und [SM-PKI-CP] stammt. ▸ [BSI.30002.8] [REQ.WAN.TlsSicherung.40]
- Das SMGW **MUSS** den TLS-Handshake beenden, sofern das vom Kommunikationspartner im TLS-Handshake empfangene Zertifikat nicht dem über ▸peerCerts bestimmten TLS-Zertifikat entspricht. [REQ.WAN.Kommunikationsprofil.41]

Schließen von TLS-Verbindungen



REQ.WAN.Transport.80

Das SMGW **MUSS** die TLS-Verbindung gemäß Parametern des zugeordneten WAN-Kommunikationsprofils beenden, falls

- ▸outboundConnection.keepOpen "false" ist und eine HTTP-Response vollständig vom Kommunikationspartner empfangen wurde bzw. an den Kommunikationspartner übermittelt wurde
- ▸outboundConnection.keepOpen "false" ist und innerhalb von ▸outboundConnection.serviceTimeout die Übermittlung einer HTTP-Response nicht begonnen wurde.
- Die maximale Lebensdauer der TLS-Sitzung ▸outboundConnection.maxSessionDuration erreicht wurde und die erfolgreiche Vereinbarung neuer TLS-Sitzungsschlüssel mit TLS1.3 innerhalb der bestehenden TLS-Verbindung nicht erfolgt ist.
- Eine Anforderung zum Beenden der TLS-Verbindung wird vom Kommunikationspartner empfangen.
- Das mit der TLS-Verbindung verknüpfte WAN- oder Proxy-Kommunikationsprofil wird gelöscht.
- Der GWA-Wechsel wurde mit ▸FA.DoSwitchGwa ausgelöst.

▸ [BSI.8002.0] ▸ [BSI.8002.1] ▸ [BSI.9002.0] ▸ [BSI.9002.1] ▸ [BSI.9004.0] ▸ [BSI.9004.1] ▸ [BSI.9006.0] ▸ [BSI.9006.1] ▸ [BSI.9008.0] ▸ [BSI.9008.1]

4.2.5 WAN-Netzwerk-Schnittstelle

- Das SMGW **MUSS** das IPv4-Protokoll an der WAN-Schnittstelle für die TLS-Verbindungen zum GWA und EMT verwenden können. [REQ.WAN.Transport.20]
- Das SMGW **SOLL** das IPv6-Protokoll an der WAN-Schnittstelle für die TLS-Verbindungen zum GWA und EMT verwenden können. (▸ICS.WAN.Transport.30) [REQ.WAN.Transport.30]

- Das SMGW **SOLL** den IPv6-Adressbezug an der WAN-Schnittstelle mittels SLAAC unterstützen. (▸ICS.WAN.Transport.30) [REQ.WAN.Transport.31]
- Das SMGW **MUSS** mindestens eine physische, von HAN und LMN getrennte Schnittstelle besitzen, die den Zugang mit einer leistungsfähigen Fernkommunikationstechnik für die WAN-Kommunikationsszenarien gemäß ▸Tabelle 4.1 mit IP-Protokollen und routbaren IP-Adressen ermöglicht. [REQ.WAN.Transport.60]

Ob eine Verbindung zum Kommunikationspartner mit IPv4 oder IPv6 Protokoll aufgebaut wird, hängt von der Adresskonfiguration (URI) ▸outboundConnection.addresses im WAN-Kommunikationsprofil und von der Konfiguration zum WAN-Zugangsnetzwerk ab (Siehe ▸hostIpv4Addr und ▸hostIpv6Addr).

ICS



ICS.WAN.Transport.20

Der GWH **MUSS** im ICS deklarieren, welches Verfahren zur Vermeidung der Überlastung von GWA-Servern durch Gleichzeitigkeitseffekte implementiert ist.



ICS.WAN.Transport.30

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



ICS.WAN.Transport.40

Der GWH **MUSS** im ICS deklarieren, ob das SMGW die TLS-ServerName Indication aus dem WAN-Kommunikationsprofil übermittelt.

4.2.6 Implementierungshinweise

Gemäß [RFC5280] soll das SMGW bei Verwendung eines TLS-Zertifikates zur Authentisierung des Kommunikationspartners prüfen, ob das Zertifikat und somit das zugehörige Schlüsselpaar gültig ist. Diese Prüfung erfolgt nach erfolgreicher Zeitsynchronisation mit der Systemzeit des SMGW. Sofern noch keine Synchronisation stattgefunden hat, wird zunächst eine Zeitsynchronisation mit dem Zeitserver (des GWA) durchgeführt. In diesem Fall wird die Authentizität des GWA-Zeitservers über das im SMGW vorliegende GWA_WAN_TLS_CRT ohne Verwendung der Systemzeit geprüft. Das SMGW kann die Plausibilisierung der zeitlichen Gültigkeit des präsentierten GWA-Zertifikates beispielsweise mit einem zuvor persistierten Zeitpunkt eines Spannungsausfalles oder Logbuch-Eintrages durchführen.

Die Zeitsynchronisation mit dem GWA soll nicht durch eine ungültige Systemzeit verhindert werden.

Es wird empfohlen TLS1.3 für künftige Implementierungen vorzusehen (siehe [DS] Kapitel "TLS"). Das TLS-1.3-Protokoll lässt eine Erneuerung der Sitzungsschlüssel bei bestehender Verbindung zu. Ein Verbindungsabbau/Aufbau ist zur Erneuerung der Sitzungsschlüssel nicht notwendig.

4.2.7 Kommunikationsszenario WKS.MANAGEMENT: Webservice-Dienste des SMGW für den GWA

4.2.7.1 Beschreibung

Das WKS.MANAGEMENT fasst die Protokolle und Nachrichtenformate zusammen, über die das SMGW an seiner WAN-Schnittstelle Dienste anbietet, damit der GWA auf diese Dienste zugreifen kann.

Diese KS besteht aus folgenden Protokollen:

- Verbindungsorientiertes Transportprotokoll TCP mit vom SMGW abgehenden Verbindungen um eine zuverlässige Übertragung zu gewährleisten.
- TLS für das SMGW in der Rolle des Clients, um vertrauliche und authentische Transportverbindungen zwischen SMGW und einem Kommunikationspartner zu gewährleisten.
- HTTP für das SMGW in der Rolle des Servers, um die Management-Webservices anzubieten.
- (optional) CMS mit dem SMGW in der Rolle des CMS-Originators und des CMS-Recipients für die Inhaltsdatensicherung zum GWA.

Das SMGW bietet dem GWA seine Dienste über ein Webservice-API gemäß [VDE0418-63-8] an. Dem Webservice-Zugriff über HTTP liegt das REST-Konzept zugrunde, bei dem ein uniformer (kleiner) Satz von Zugriffs-Verben auf verschiedene Ressourcen angewandt werden kann (Create, Read, Update, Delete). Die Ressourcen können jeweils von unterschiedlichem Inhaltstyp (Content-Type) sein. Darüber hinaus bietet das SMGW Dienste zum Aufruf von Funktionen über das Webservice-API an.

Das SMGW nimmt keine eingehenden Verbindungen an der WAN-Schnittstelle an. Stattdessen baut das SMGW eine Transport-Verbindung zum GWA auf und führt den TLS-Handshake in der Rolle des TLS-Client aus. Es bietet anschließend seine Dienste als HTTP-Server an.

▸Abbildung 4.3 verdeutlicht den Ablauf der im WKS.MANAGEMENT verwendeten Kommunikationsdienste TLS-Verbindungsaufbau, Aufruf des Webservice-Dienstes durch den GWA und TLS-Verbindungsabbau.

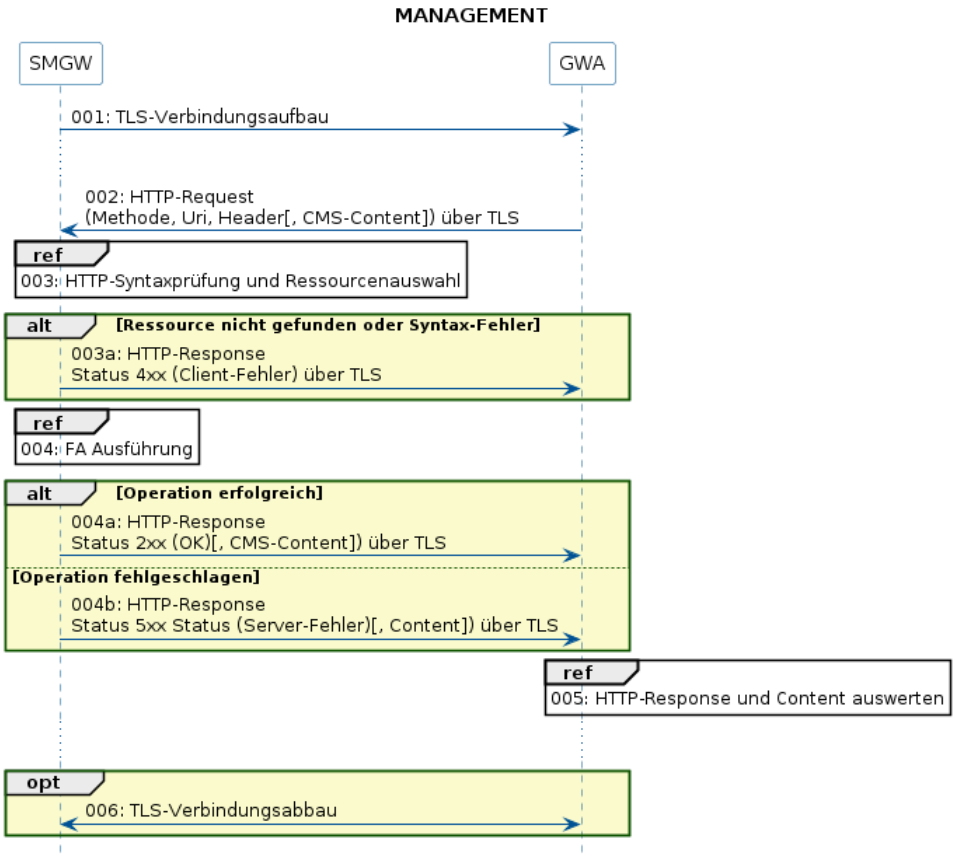


Abbildung 4.3. Übersicht über den Ablauf des WKS.MANAGEMENT

4.2.7.2 Vorbedingungen

Der GWA ist für das SMGW kommunikativ erreichbar.

Die Kommunikationsadresse des GWA-Kommunikationssystems, das akzeptierte TLS-Server-Zertifikat des GWA_WAN_TLS_CRT, das Verschlüsselungszertifikat GWA_WAN_ENC_CRT und das GWA_WAN_SIG_CRT liegen im SMGW vor.

4.2.7.3 Technische Anwendungsfälle der Kommunikationsprotokolle

Das Kommunikationsszenario WKS.MANAGEMENT verwendet die in ▸Tabelle 4.2 beschriebenen technischen Anwendungsfälle der Kommunikationsprotokolle mit den über ein WAN-Kommunikationsprofil vom Typ "MANAGEMENT" definierten Parametern.

Aufgabe	Detailspezifikation	Parameter
Aktives Öffnen einer Transport-Verbindung (abgehende Verbindung)	TCP gemäß [RFC9293]	Das SMGW **MUSS** eine TCP-Verbindung gemäß [RFC9293] in der Rolle des Initiators (Active Opener) zur ersten der in ▸outboundConnection.addresses angegebenen Transport-Adressen über die Schnittstelle gemäß ▸outboundConnection.ifName initiieren. [REQ.WKS.MANAGEMENT.10]

Aufgabe	Detailspezifikation	Parameter
Öffnen einer TLS-Session als Client	[DS] Kapitel "TLS" TA.TLS.OpenWanSessionAsClient, TA.TLS.Handshake	Anforderungen an die TLS-Authentifizierung zwischen SMGW und GWA-Kommunikationssystem sind in ▸Abschnitt 4.2.4 beschrieben. Das SMGW **MUSS** TLS gemäß [DS] Kapitel "TLS" in der Rolle des Clients verwenden. [REQ.WKS.MANAGEMENT.20] Das SMGW **MUSS** die TLS-Verbindung zum GWA mit den Parametern des WAN-Kommunikationsprofiles der Domäne "gwa-management" aufbauen. ▸ [BSI.8001.0] ▸ [BSI.8001.1] [REQ.WKS.MANAGEMENT.60]
Schließen der TCP/TLS-Verbindung nach Empfang eines Close-Notify Alerts	[DS] Kapitel "TLS" TA.TLS.Close	Siehe ▸REQ.WAN.Transport.80
Schließen der TCP/TLS-Verbindung, initiiert durch das SMGW		
Verarbeiten einer HTTP-Anfrage	[DS] Kapitel "RESTful Webservice" Anforderungen an HTTP-Server	Das SMGW **MUSS** HTTP gemäß [DS] Kapitel "RESTful Webservice" in der Rolle des Servers verwenden. [REQ.WKS.MANAGEMENT.30]
Erzeugen einer HTTP-Antwort		Das SMGW **MUSS** den Zugriff auf Ressourcen des SMGW über das Kommunikationsszenario WKS MANAGEMENT mit einem RESTful Webservice Protokoll gemäß [DS] Kapitel "RESTful Webservice" umsetzen. [REQ.WAN.Webservice.10] Das SMGW **MUSS** Fehler beim Zugriff auf eine (Webservice)-Ressource unmittelbar mit einer HTTP-Response gemäß [DS] Kapitel "RESTful Webservice" Abschnitt "Status Codes" beantworten. ▸ [BSI.2002.1] [REQ.WAN.Webservice.20] Das SMGW **MUSS** in der Webservice-Response mitteilen, welchen Content-Type (Struktur, Transfersyntax) die Inhaltsdaten besitzen. [REQ.WAN.Webservice.60] Das SMGW **SOLL** innerhalb der "Service Timeout"-Zeit gemäß WAN-Kommunikationsprofil eine HTTP-Anfrage beantworten. [REQ.WAN.Webservice.70] Das SMGW **MUSS+** den Zugriff auf Ressourcen der FA, die über WKS.MANAGEMENT ausgelöst werden, mit Verb, URI, Header, Status-Response, Request-Content und Response-Content gemäß Anlage Webservice-API - SMGW-API 2.0 für den GWA implementieren. (▸ICS.WKS.MANAGEMENT.20) [REQ.WAN.Webservice.90] Das SMGW **MUSS** das Löschen einer Ressource (FA.Delete...) ablehnen, wenn die über die URI identifizierte Ressource (URI) nicht im SMGW existiert. [REQ.WAN.Webservice.120]
Verarbeiten einer CMS-Nachricht	[DS] Kapitel "CMS"	Sofern der HTTP-Request-Inhalt gemäß Content-Type Header (siehe [DS] Kapitel "RESTful Webservice" Abschnitt "Content Type") mit CMS übertragen wird, **MUSS** das SMGW die Nachricht gemäß [DS] Kapitel "CMS" als Recipient verarbeiten. ▸ [BSI.4001.1] [REQ.WKS.MANAGEMENT.40] Das SMGW **MUSS** empfangene CMS-Nachrichten verwerfen, deren Signatur nicht mit dem Signatur-Zertifikat aus ▸peerCerts validiert werden kann. ▸ [BSI.4002.1] ▸ [BSI.4002.2] ▸ [BSI.4002.3] [REQ.WAN.CmsSicherung.30] Das SMGW **MUSS** empfangene CMS-Nachrichten verwerfen, für die kein administrativ konfiguriertes GW_WAN_ENC_CRT im SMGW vorliegt oder die nicht den Anforderungen gemäß [DS] Kapitel "CMS" als Recipient entsprechen. ▸ [BSI.4004.1] ▸ [BSI.4004.2] [REQ.WAN.CmsSicherung.31]

Aufgabe	Detailspezifikation	Parameter
Erzeugen einer CMS-Nachricht	[DS] Kapitel "CMS"	Sofern der HTTP-Client des Kommunikationspartners gemäß Accept-Header (siehe [DS] Kapitel "RESTful Webservice" Abschnitt "Content Type") die HTTP-Response des SMGW mit CMS-Inhaltsdatensicherung erwartet, **MUSS** das SMGW die Nachricht gemäß [DS] Kapitel "CMS" als Originator erzeugen. (▸ICS.WKS.MANAGEMENT.10) [REQ.WKS.MANAGEMENT.50] Sofern der HTTP-Response Content verschlüsselt an den GWA übermittelt wird, **MUSS** das SMGW die Nachricht für den GWA mit dem GWA_WAN_ENC_CRT-Zertifikat aus ▸peerCerts verschlüsseln. [REQ.WKS.MANAGEMENT.70]
Verarbeiten einer Applikations-Nachricht	[DS] Kapitel "RESTful Webservice"	Das SMGW **MUSS+** Webservice-Requests auf Ressourcen gemäß Anlage Webservice-API - SMGW-API 2.0 für den GWA, die nicht der Transfer-Syntax und dem Schema für diese Ressource entsprechen, unmittelbar mit einer Webservice-Response gemäß [DS] Kapitel "RESTful Webservice" Abschnitt "Status Codes" ablehnen.(▸ICS.WKS.MANAGEMENT.20) [REQ.WAN.Webservice.100] Das SMGW **MUSS** das Anlegen einer Ressource (FA.Create...) ablehnen, wenn die Ressource ein Datenfeld "profileId" enthält, das dem Datenfeld "profileId" einer bereits im SMGW existierenden Ressource entspricht. [REQ.WAN.Webservice.130] Das SMGW **MUSS** eine Aktualisierung einer Ressource (FA.Update...) ablehnen, wenn die Ressource ein Datenfeld "profileId" enthält, dessen Inhalt nicht der Ressource-Identifikation (URI) entspricht. [REQ.WAN.Webservice.110]
Erzeugen einer Applikations-Nachricht		Das SMGW **MUSS+** die Applikations-Nachricht mit Syntax und Struktur gemäß Anlage Webservice-API - SMGW-API 2.0 für den GWA für die Ressource erzeugen.(▸ICS.WKS.MANAGEMENT.20) [REQ.WKS.MANAGEMENT.90]

Tabelle 4.2 Übersicht der TA des WKS.MANAGEMENT



ICS.WKS.MANAGEMENT.10

Der GWH **MUSS** im ICS beschreiben, welche Verfahren und Parameter das SMGW beim Versand von CMS-Nachrichten mittels MANAGEMENT verwendet. Es muss mindestens die CMS_Z-LIB-Kompression, CMS_ECDSA_SHA256-Signatur und eines der CMS_ECKAEG_AES-Verschlüsselungsverfahren ausgewählt werden.



ICS.WKS.MANAGEMENT.20

Der GWH **MUSS** im ICS deklarieren, welches Datenformat für die Applikationsnachrichten beim Empfang und Versand mittels MANAGEMENT verwendet wird.

4.2.8 Kommunikationsszenario WKS.ADMIN-SERVICE: Aufruf von Anwendungsdiensten des GWA mit dem SMGW als Webservice-Client

4.2.8.1 Beschreibung

Das WKS.ADMIN-SERVICE fasst die Protokolle und Nachrichtenformate zusammen, über die das SMGW an seiner WAN-Schnittstelle Anwendungsdienste der Kommunikationssysteme des GWA aufrufen kann.

Dieses KS besteht aus folgenden Protokollen:

- Verbindungsorientiertes Transportprotokoll TCP mit vom SMGW abgehenden Verbindungen um eine zuverlässige Übertragung zu gewährleisten.
- TLS für das SMGW in der Rolle des Clients, um vertrauliche und authentische Transportverbindungen zwischen SMGW und einem Kommunikationspartner zu gewährleisten.
- HTTP für RESTful Webservices für das SMGW in der Rolle des Clients, um die Webservices des GWA aufzurufen.

- (optional) CMS in der Rolle des CMS-Originators für die Inhaltsdatensicherung zum GWA.

Der Benachrichtigung des GWA wird beispielsweise gemäß ▸FA.DoEventNotification ausgelöst.

Die Informationssysteme des GWA bieten dem SMGW ihre Dienste über ein Webservice-API an. Das SMGW kann diese Dienste über das WKS.ADMIN-SERVICE aufrufen.

▸Abbildung 4.4 verdeutlicht den Ablauf der im WKS.ADMIN-SERVICE verwendeten Kommunikationsdienste TLS-Verbindungsaufbau, Aufruf des Webservice-Dienstes durch das SMGW und TLS-Verbindungsabbau.

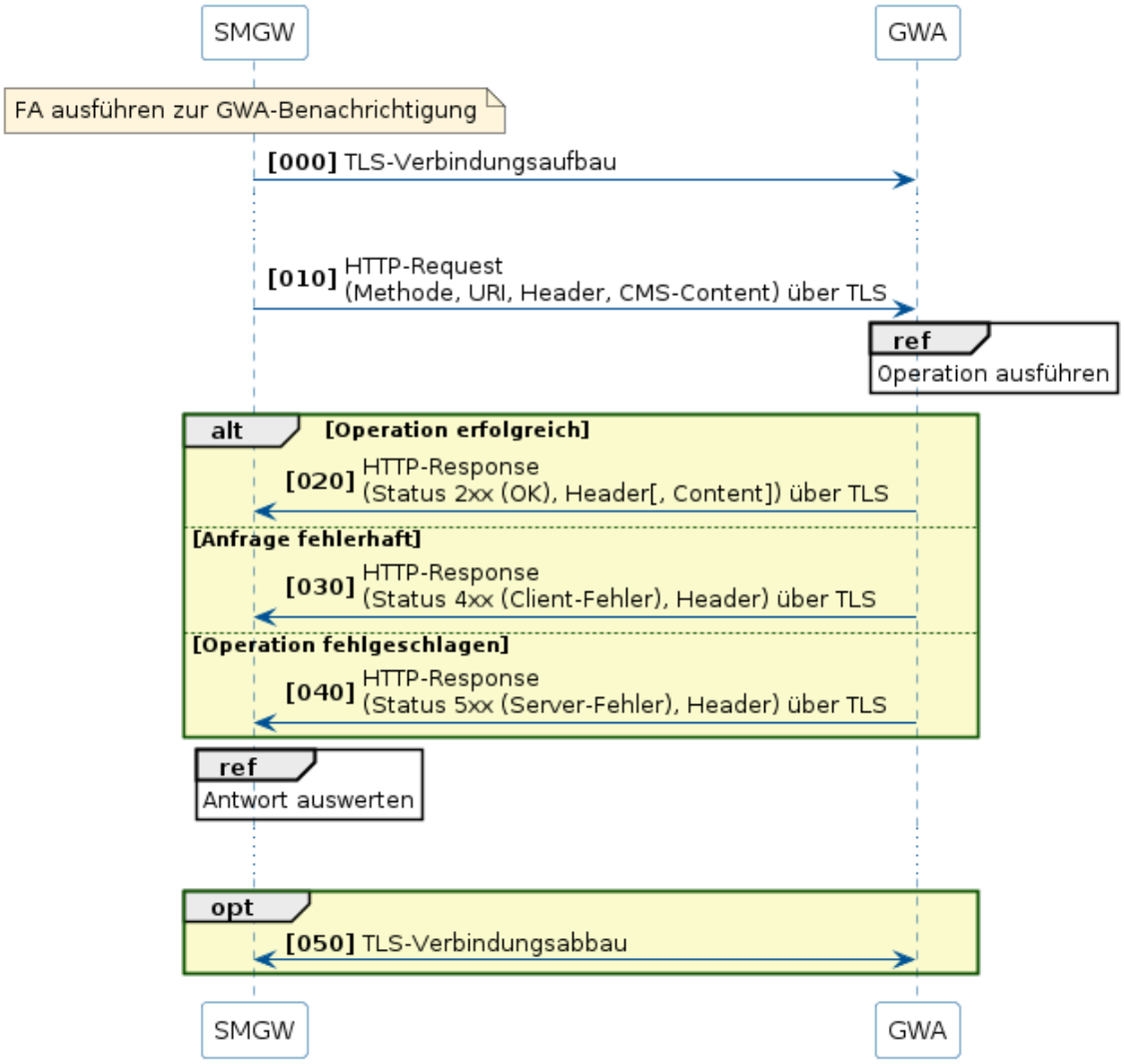


Abbildung 4.4. Übersicht über den Ablauf des WKS.ADMIN-SERVICE

4.2.8.2 Vorbedingungen

Der GWA ist für das SMGW kommunikativ erreichbar.

Die Kommunikationsadresse des GWA-Kommunikationssystems, das akzeptierte TLS-Server-Zertifikat des GWA_WAN_TLS_CRT, das Verschlüsselungszertifikat GWA_WAN_ENC_CRT und das GWA_WAN_SIG_CRT liegen im SMGW vor.

4.2.8.3 Anforderungen an die Kommunikationsprotokolle

Das Kommunikationsszenario WKS.ADMIN-SERVICE verwendet die in ▸Tabelle 4.3 beschriebenen technischen Anwendungsfälle der Kommunikationsprotokolle mit den über ein WAN-Kommunikationsprofil vom Typ "ADMIN-SERVICE" definierten Parametern.

Aufgabe	Detailspezifikation	Parameter
Aktives Öffnen einer Transport-Verbindung (abgehende Verbindung)	TCP gemäß [RFC9293]	Das SMGW **MUSS** eine TCP-Verbindung gemäß [RFC9293] in der Rolle des Initiators (Active Opener) zur ersten der in ▸outboundConnection.addresses angegebenen Transport-Adressen über die Schnittstelle gemäß ▸outboundConnection.ifName initiieren. [REQ.WKS.ADMIN-SERVICE.10]
Öffnen einer TLS-Session als Client	[DS] Kapitel "TLS" TA.TLS.OpenWanSessionAsClient, TA.TLS.Handshake	Anforderungen an die TLS-Authentifizierung zwischen SMGW und GWA-Kommunikationssystem sind in ▸Abschnitt 4.2.4 beschrieben. Das SMGW **MUSS** TLS gemäß [DS] Kapitel TLS in der Rolle des Clients verwenden. [REQ.WKS.ADMIN-SERVICE.20] (GWA-Wechsel nicht aktiv: ▸FA.DoSwitchGwa nicht aufgerufen oder ▸FA.AcceptSwitchGwa aufgerufen) Das SMGW **MUSS** die TLS-Verbindung zum GWA mit den Parametern des WAN-Kommunikationsprofiles der Domäne "gwa-adminservice" aufbauen, ▸ [BSI.9001.0] ▸ [BSI.9001.1] [REQ.WKS.ADMIN-SERVICE.50] (GWA-Wechsel aktiv: ▸FA.DoSwitchGwa gestartet und ▸FA.AcceptSwitchGwa nicht erfolgt) Das SMGW **MUSS** die TLS-Verbindung zum GWA mit den Parametern des WAN-Kommunikationsprofiles der Domäne "gwapre-adminservice" aufbauen, ▸ [BSI.9001.0] ▸ [BSI.9001.1] [REQ.WKS.ADMIN-SERVICE.51]
Schließen der TCP/TLS-Verbindung nach Empfang eines Close-Notify Alerts	[DS] Kapitel "TLS" TA.TLS.Close	Siehe ▸REQ.WAN.Transport.80
Schließen der TCP/TLS-Verbindung, initiiert durch das SMGW		
Senden einer HTTP-Anfrage	[DS] Kapitel "RESTful Webservice" Anforderungen an HTTP-Clients	Das SMGW **MUSS** HTTP gemäß [DS] Kapitel RESTful Webservice in der Rolle des Clients verwenden. [REQ.WKS.ADMIN-SERVICE.30] (▸messageFormat.omitCms gleich "true") Das SMGW **MUSS** den HTTP "message-body" gemäß [DS] Kapitel "RESTful Webservice" komprimieren. [REQ.WKS.ADMIN-SERVICE.31] Das SMGW **MUSS** Nachrichten über WKS.ADMIN-SERVICE an den GWA mittels HTTP "POST" Request an die erste URI ▸outboundConnection.addresses des WAN-Kommunikationsprofils bereitstellen. [REQ.WKS.ADMIN-SERVICE.60] Das SMGW **MUSS**+ den Zugriff auf Ressourcen des GWA, die über WKS.ADMIN-SERVICE ausgelöst werden, mit Verb, URI, Header, Status-Response, Request-Content und Response-Content gemäß Anlage Webservice-API - GWA-API 2.0 für das SMGW implementieren. (▸ICS.WKS.ADMIN-SERVICE.20) [REQ.WKS.ADMIN-SERVICE.70]
Erzeugen einer CMS-Nachricht	[DS] Kapitel "CMS"	(▸messageFormat.omitCms gleich "false") Das SMGW **MUSS** gemäß [DS] Kapitel "CMS" als Originator Inhaltsdaten für den GWA komprimieren, verschlüsseln und signieren. (▸ICS.WKS.ADMIN-SERVICE.10) [REQ.WKS.ADMIN-SERVICE.40] Inhaltsdaten einer HTTP-Nachricht sind die Daten im "message-body" (auch als "Content" bezeichnet).
Verarbeiten einer HTTP-Antwort	[DS] Kapitel "RESTful Webservice" Anforderungen an HTTP-Clients	Das SMGW **MUSS** bis zu ▸outboundConnection.serviceTimeout Sekunden auf eine HTTP-Antwort warten ▸ [BSI.2003.1] . [REQ.WKS.ADMIN-SERVICE.80] Das SMGW **MUSS** den Statuscode der HTTP-Response protokollieren. ▸ [BSI.2003.2] ▸ [BSI.2003.0] [REQ.WKS.ADMIN-SERVICE.100] Das SMGW verarbeitet empfangene Nachrichten gemäß Content-Type-Header (siehe [DS] Kapitel "RESTful Webservice" Abschnitt "Content Type").

Aufgabe	Detailspezifikation	Parameter
Erzeugen einer Applikations-Nachricht	[DS] Kapitel "RESTful Webservice"	Das SMGW **MUSS+** die Applikations-Nachricht mit Syntax und Struktur gemäß Anlage Webservice-API - GWA-API 2.0 für das SMGW für die Ressource erzeugen.(▸ICS.WKS.ADMIN-SERVICE.20) [REQ.WKS.ADMIN-SERVICE.110]

Tabelle 4.3 Anforderungen an die Protokolllayer des WKS.ADMIN-SERVICE

ICS



ICS.WKS.ADMIN-SERVICE.10

Der GWH **MUSS** im ICS beschreiben, welche Verfahren und Parameter das SMGW beim Versand von CMS-Nachrichten mittels ADMIN-SERVICE verwendet. Es muss mindestens die CMS_ZLIB-Kompression, CMS_ECDSA_SHA256-Signatur und eines der CMS_ECKAEG_AES-Verschlüsselungsverfahren ausgewählt werden.



ICS.WKS.ADMIN-SERVICE.20

Der GWH **MUSS** im ICS deklarieren, welches Datenformat für die Applikationsnachrichten beim Versand mittels ADMIN-SERVICE verwendet wird.

4.2.9 Kommunikationsszenario WKS.INFO-REPORT: Nachrichtenübermittlung an EMT mit dem SMGW als Webservice-Client

4.2.9.1 Beschreibung

Das WKS.INFO-REPORT fasst die Protokolle und Nachrichtenformate zusammen, über die das SMGW an seiner WAN-Schnittstelle Inhaltsdaten (Messwerte) an einen berechtigten EMT übermittelt.

Vom EMT empfangene Inhaltsdaten werden vom SMGW nicht verarbeitet, ausgenommen sind Statusinformationen zur Zustellung der Nachricht.

Dieses KS besteht aus folgenden Protokollen:

- Verbindungsorientiertes Transportprotokoll TCP mit vom SMGW abgehenden Verbindungen um eine zuverlässige Übertragung zu gewährleisten.
- TLS für das SMGW in der Rolle des Clients um vertrauliche und authentische Transportverbindungen zwischen SMGW und EMT zu gewährleisten.
- HTTP für das SMGW in der Rolle des Clients, um die Webservices des EMT aufzurufen.
- (optional) CMS mit dem SMGW in der Rolle des CMS-Originators für die Inhaltsdatensicherung zum EMT.

Der Nachrichtenversand wird gemäß ▸FAKAT.ValTransmission ausgelöst.

Die Informationssysteme des EMT oder GWA bieten dem SMGW die Nachrichtenzustellung über ein Webservice-API an.

▸Abbildung 4.5 und ▸Abbildung 4.6 verdeutlichen den Ablauf der im WKS.INFO-REPORT verwendeten Kommunikationsdienste TLS-Verbindungsaufbau, Aufruf des Webservice-Dienstes durch das SMGW und TLS-Verbindungsabbau.

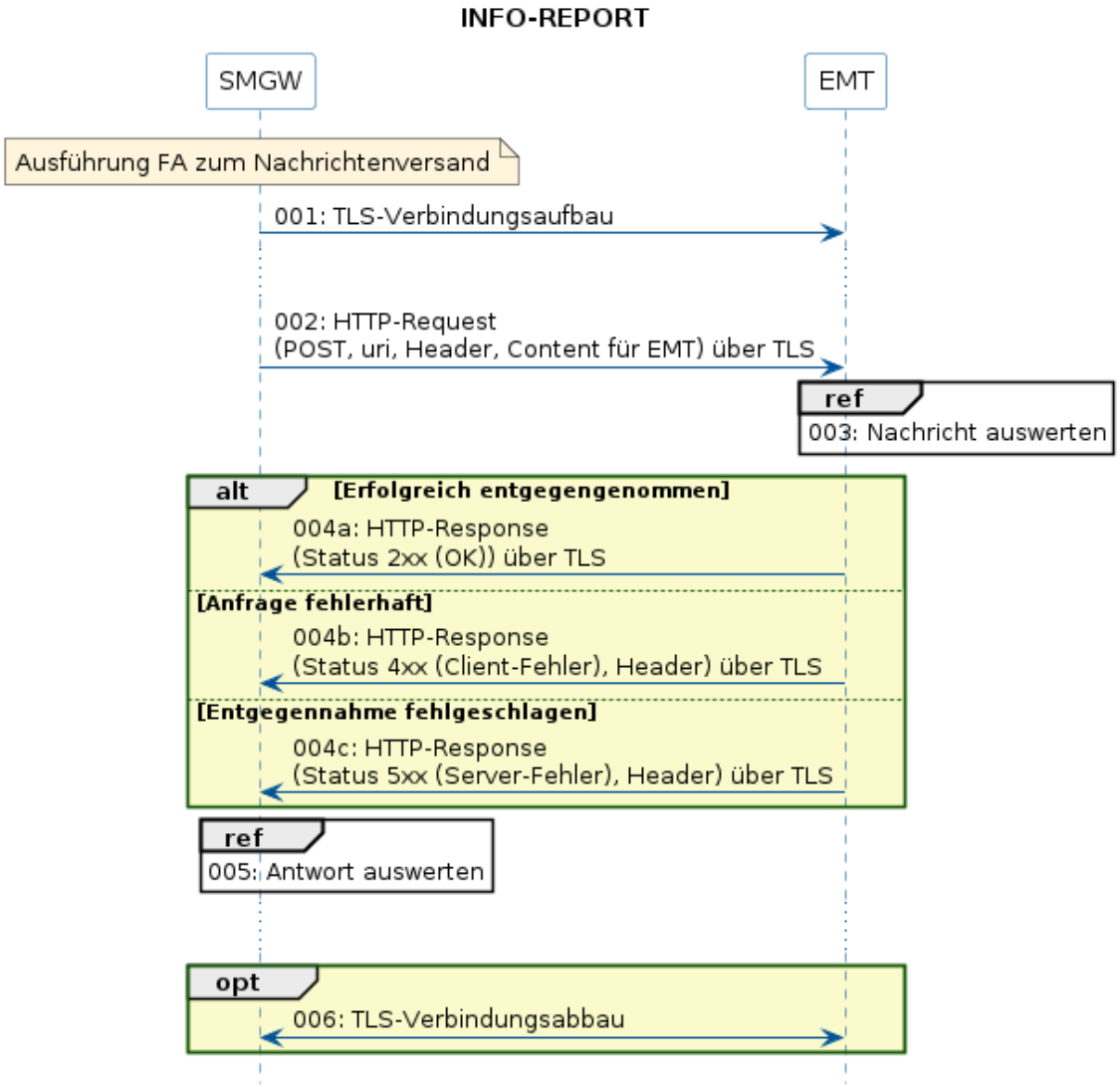


Abbildung 4.5. Übersicht über den Ablauf des WKS.INFO-REPORT zum EMT

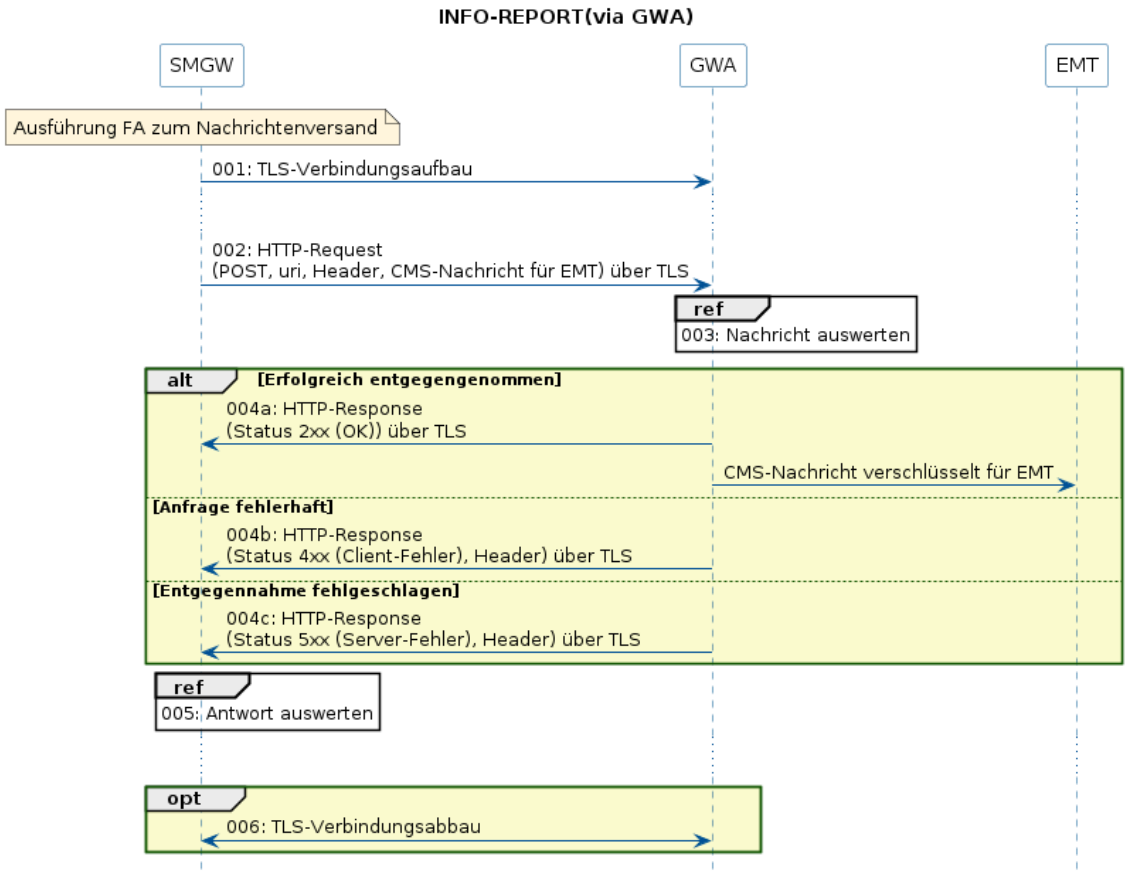


Abbildung 4.6. Übersicht über den Ablauf des WKS.INFO-REPORT via GWA

4.2.9.2 Vorbedingungen

Der EMT ist für das SMGW kommunikativ erreichbar.

Die Kommunikationsadresse des EMT, das akzeptierte TLS-Server-Zertifikat EMT_WAN_TLS_CRT bzw. GWA_WAN_TLS_CRT und das Verschlüsselungszertifikat EMT_WAN_ENC_CRT liegen im SMGW vor.

4.2.9.3 Anforderungen an die Kommunikationsprotokolle

Das Kommunikationsszenario WKS.INFO-REPORT verwendet die in ▸Tabelle 4.4 beschriebenen technischen Anwendungsfälle der Kommunikationsprotokolle mit den über ein WAN-Kommunikationsprofil vom Typ "INFO-REPORT" definierten Parametern.

Aufgabe	Detailspezifikation	Parameter
Aktives Öffnen einer Transport-Verbindung (abgehende Verbindung)	TCP gemäß [RFC9293]	Das SMGW **MUSS** eine TCP-Verbindung gemäß [RFC9293] in der Rolle des Initiators (Active Opener) zur ersten der in ▸outboundConnection.addresses angegebenen Transport-Adressen über die Schnittstelle gemäß ▸outboundConnection.ifName initiieren. [REQ.WKS.INFO-REPORT.10]

Aufgabe	Detailspezifikation	Parameter
Öffnen einer TLS-Session als Client	[DS] Kapitel "TLS" TA.TLS.OpenWanSessionAsClient, TA.TLS.Handshake	Anforderungen an die TLS-Authentifizierung zwischen SMGW und EMT-Kommunikationssystem sind in ▸Abschnitt 4.2.4 beschrieben. Das SMGW **MUSS** TLS gemäß [DS] Kapitel TLS in der Rolle des Clients verwenden. [REQ.WKS.INFO-REPORT.20] Sofern im auslösenden Auswertungsprofil ▸meterDataOutput.viaGwa "false" ist **MUSS** das SMGW die TLS-Verbindung zum EMT mit den Parametern des WAN-Kommunikationsprofiles vom Typ ▸wks gleich "INFO-REPORT" aufbauen, dessen ▸peerCerts *SubjectCN* (EMT-ID) der ▸meterDataOutput.wanPeerRef im auslösenden Auswertungsprofil entspricht. ▸ [BSI.9003.0] ▸ [BSI.9003.1] [REQ.WKS.INFO-REPORT.50] Sofern im auslösenden Auswertungsprofil ▸meterDataOutput.viaGwa "true" ist **MUSS** das SMGW die TLS-Verbindung zum GWA mit den Parametern des WAN-Kommunikationsprofiles der Domäne "gwa-adminservice" aufbauen und die Nachrichten mit den Parametern des WAN-Kommunikationsprofils vom Typ ▸wks "INFO-REPORT" für den EMT verschlüsseln, dessen ▸peerCerts EMT_WAN_TLS_CRT *SubjectCN* (EMT-ID) der ▸meterDataOutput.wanPeerRef im auslösenden Auswertungsprofil entspricht. ▸ [BSI.9001.0] ▸ [BSI.9001.1] [REQ.WKS.INFO-REPORT.51] Beim Anlegen und Aktualisieren des EMT-WAN-Kommunikationsprofils wird gewährleistet, dass eine Nachrichtenverschlüsselung konfiguriert ist.
Schließen der TCP/TLS-Verbindung nach Empfang eines Close-Notify Alerts	[DS] Kapitel "TLS" TA.TLS.Close	Siehe ▸REQ.WAN.Transport.80
Schließen der TCP/TLS-Verbindung, initiiert durch das SMGW		
Senden einer HTTP-Anfrage	[DS] Kapitel "RESTful Webservice" Anforderungen an HTTP-Clients	Das SMGW **MUSS** HTTP gemäß [DS] Kapitel RESTful Webservice in der Rolle des Clients verwenden. [REQ.WKS.INFO-REPORT.30] (▸messageFormat.omitCms gleich "true") Das SMGW **MUSS** den HTTP "message-body" gemäß [DS] Kapitel "RESTful Webservice" komprimieren. [REQ.WKS.INFO-REPORT.31] Das SMGW **MUSS** Nachrichten über WKS.INFO-REPORT an den EMT oder GWA mittels HTTP "POST"-Request an die erste URI ▸outboundConnection.addresses des für den Transport verwendeten WAN-Kommunikationsprofils bereitstellen. [REQ.WAN.Webservice.50] Das SMGW **MUSS**+ den Zugriff auf EMT-Ressourcen, die über WKS.INFO-REPORT ausgelöst werden, mit Verb, URI, Header, Status-Response, Request-Content und Response-Content gemäß Anlage Webservice-API - EMT-API 2.0 für das SMGW implementieren. [REQ.WKS.INFO-REPORT.70]

Aufgabe	Detailspezifikation	Parameter
Erzeugen einer CMS-Nachricht	[DS] Kapitel "CMS"	Das SMGW **MUSS** Inhaltsdaten für den Endempfänger gemäß [DS] Kapitel "CMS" als Originator komprimieren, verschlüsseln und signieren. (▸ICS.WKS.INFO-REPORT.10) [REQ.WKS.INFO-REPORT.40] Inhaltsdaten einer HTTP-Nachricht sind die Daten im "message-body" (auch als "Content" bezeichnet). Sofern im auslösenden Auswertungsprofil ▸meterDataOutput.viaGwa "true" ist oder im WAN-Kommunikationsprofil ▸messageFormat.omitCms "false" ist **MUSS** das SMGW die Nachrichten mit den Parametern des WAN-Kommunikationsprofils vom Typ ▸wks "INFO-REPORT" für den EMT mit dem Schlüssel aus ▸peerCerts.encCert verschlüsseln. Das WAN-Kommunikationsprofil wird über ▸meterDataOutput.wanPeerRef des auslösenden Auswertungsprofils identifiziert. [REQ.WKS.INFO-REPORT.52] Beim Anlegen und Aktualisieren des Auswertungsprofils mit "viaGwa" gleich "true" wird gewährleistet, dass eine Nachrichtenverschlüsselung konfiguriert ist. Sofern im auslösenden Auswertungsprofil ▸meterDataOutput.viaGwa gleich "false" ist und im EMT-WAN-Kommunikationsprofil ▸messageFormat.omitCms "true" ist **MUSS** das SMGW die Inhaltsdaten ohne CMS-Envelope senden. [REQ.WKS.INFO-REPORT.53] Dies ist möglich, da die Daten bis zum Endempfänger mittels TLS gesichert sind.
Verarbeiten einer HTTP-Antwort	[DS] Kapitel "RESTful Webservice" Anforderungen an HTTP-Clients	Das SMGW **MUSS** bis zu ▸outboundConnection.serviceTimeout Sekunden auf eine HTTP-Antwort warten ▸ [BSI.2003.1] . [REQ.WKS.INFO-REPORT.60] Das SMGW **MUSS** den Statuscode der HTTP-Response protokollieren. ▸ [BSI.2003.2] ▸ [BSI.2003.0] [REQ.WKS.INFO-REPORT.90] Das SMGW verarbeitet empfangene Nachrichten gemäß Content-Type-Header (siehe [DS] Kapitel "RESTful Webservice" Abschnitt "Content Type").
Erzeugen einer Applikations-Nachricht	[DS] Kapitel "RESTful Webservice"	Das SMGW **MUSS**+ die Applikations-Nachricht mit Syntax und Struktur gemäß Anlage Webservice-API - EMT-API 2.0 für das SMGW für die Ressource erzeugen.(▸ICS.WKS.INFO-REPORT.20) [REQ.WKS.INFO-REPORT.100]

Tabelle 4.4 Anforderungen an die Protokolllayer des WKS.INFO-REPORT

ICS



ICS.WKS.INFO-REPORT.10

Der GWH **MUSS** im ICS beschreiben, welche Verfahren und Parameter das SMGW beim Versand von CMS-Nachrichten mittels INFO-REPORT verwendet. Es muss mindestens die CMS_ZLIB-Kompression, CMS_ECDSA_SHA256-Signatur und eines der CMS_ECKAEG_AES-Verschlüsselungsverfahren ausgewählt werden.



ICS.WKS.INFO-REPORT.20

Der GWH **MUSS** im ICS deklarieren, welches Datenformat für die Applikationsnachrichten beim Versand mittels INFO-REPORT verwendet wird.

4.2.10 Kommunikationsszenario WKS.NTP-TLS: Zeitsynchronisation mit dem SMGW als NTP-TLS-Client

4.2.10.1 Beschreibung

Das WKS.NTP-TLS fasst die Protokolle und Nachrichtenformate für eine Zeitsynchronisation mittels NTP über TLS zusammen, über die das SMGW an seiner WAN-Schnittstelle die Zeitsynchronisation mit dem Zeitserver des GWA durchführt.

Dieses KS besteht aus folgenden Protokollen:

- Verbindungsorientiertes Transportprotokoll TCP/IP mit abgehenden Verbindungen.

- TLS für das SMGW in der Rolle des Clients, um vertrauliche und authentische Transportverbindungen zwischen SMGW und einem Kommunikationspartner zu gewährleisten.
- NTP für das SMGW in der Rolle des Clients, um die Nachrichten zur Zeitsynchronisation auszutauschen.

Das SMGW nutzt den Zeitserver des GWA mit den Protokollen NTP über TLS. Da eine 1:1 Zuordnung von NTP-Message und TLS-Application-Record vorliegt und darüber hinaus die NTP-Nachrichten eine feste Länge haben, ist kein Adaptionslayer zwischen NTP und TLS notwendig.

▸Abbildung 4.7 verdeutlicht den Ablauf, der im WKS.NTP-TLS verwendeten Kommunikationsdienste TLS-Verbindungsaufbau, Abfrage des Zeitservers und Verbindungsabbau.

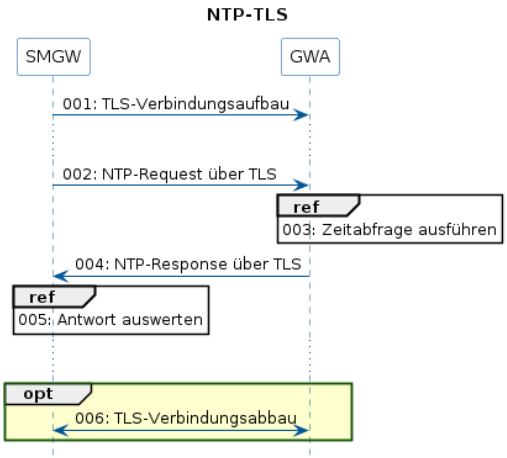


Abbildung 4.7. Übersicht über den Ablauf des WKS.NTP-TLS

4.2.10.2 Vorbedingungen

Der GWA ist für das SMGW kommunikativ erreichbar.

Die Kommunikationsadresse des GWA-Zeitservers und das den berechtigten GWA identifizierende TLS-Server-Zertifikat GWA_WAN_TLS_CRT sind durch den GWA oder im Rahmen der Vorpersonalisierung über ein WAN-Kommunikationsprofil im SMGW parametriert worden.

4.2.10.3 Anforderungen an die Kommunikationsprotokolle

Das Kommunikationsszenario WKS.NTP-TLS verwendet die in ▸Tabelle 4.5 beschriebenen technischen Anwendungsfälle der Kommunikationsprotokolle mit den über ein WAN-Kommunikationsprofil vom Typ "NTP-TLS" definierten Parametern.

Aufgabe	Detailspezifikation	Parameter
Aktives Öffnen einer Transport-Verbindung (abgehende Verbindung)	TCP gemäß [RFC9293]	Das SMGW **MUSS** die TLS-Verbindung zum GWA mit den Parametern des WAN-Kommunikationsprofiles der Domäne "gwa-ntptls" aufbauen. ▸[BSI.9005.0] ▸[BSI.9005.1] [REQ.WKS.NTP-TLS.30] Das SMGW **MUSS** eine TCP-Verbindung gemäß [RFC9293] in der Rolle des Initiators (Active Opener) zur ersten der in ▸outboundConnection.addresses angegebenen Transport-Adressen über die Schnittstelle gemäß ▸outboundConnection.ifName initiieren. [REQ.WKS.NTP-TLS.10]
Öffnen einer TLS-Session als Client	[DS] Kapitel "TLS" TA.TLS.OpenWanSessionAsClient, TA.TLS.Handshake	Anforderungen an die TLS-Authentifizierung zwischen SMGW und GWA-Kommunikationssystem sind in ▸Abschnitt 4.2.4 beschrieben. Das SMGW **MUSS** TLS gemäß [DS] Kapitel "TLS" in der Rolle des Clients verwenden. [REQ.WKS.NTP-TLS.20]
Senden von TLS-Applikationsdaten	-	Das SMGW **MUSS** die NTP-Nachrichten (Request/Response) ohne weitere vorangestellte oder nachfolgende Daten als TLS-Applikationsdaten übertragen und empfangen. [REQ.WAN.Zeitsynchronisation.70]
Empfangen von TLS-Applikationsdaten	-	

Aufgabe	Detailspezifikation	Parameter
Schließen der TCP/ TLS-Verbindung nach Empfang eines Close-Notify Alerts	[DS] Kapitel "TLS" TA.TLS.Close	Siehe ▸REQ.WAN.Transport.80
Schließen der TCP/ TLS-Verbindung, initiiert durch das SMGW		
Erzeugen einer NTP-Anfrage	[DS] Kapitel "NTP" TA.NTP.BuildRequest	Das SMGW **MUSS** die für das NTP-Protokoll notwendige Bestimmung der Sende- und Empfangszeitpunkte der NTP-Nachrichten erst durchführen, nachdem die TLS-gesicherte Verbindung aufgebaut ist, damit die Zeit, die für den Verbindungaufbau benötigt wird nicht die RTT-Messung beeinflusst. [REQ.WAN.Zeitsynchronisation.40] Das SMGW **MUSS** die Zeitsynchronisation mit den Datenstrukturen und Anforderungen an die Verarbeitung des NTP-Protokolls gemäß [DS] Kapitel "NTP" durchführen. [REQ.WAN.Zeitsynchronisation.10]
Verarbeiten einer NTP-Antwort	[DS] Kapitel "NTP" TA.NTP.ProcessResponse	

Tabelle 4.5 Anforderungen an die Protokolllayer des WKS.NTP-TLS

4.2.10.4 Implementierungshinweise

Der Inhalt des Datenfeldes ▸messageFormat wird, sofern er im WAN-Kommunikationsprofil vorhanden ist, nicht berücksichtigt.

4.2.11 Kommunikationsszenario WKS.TLSPROXY: Proxy Verbindung im WAN mit dem SMGW als TLS-Client

4.2.11.1 Beschreibung

Dieses KS dient dem authentischen und vertraulichen Austausch von Anwendungsdaten - ohne Anforderung an das Anwendungsprotokoll - zwischen einem aktiven EMT (aEMT) im WAN und einem über ein Proxy-Kommunikationsprofil berechtigten HAN-Teilnehmer (CLS).

Das WKS.TLSPROXY fasst die Protokolle zusammen, mit denen das SMGW über eine Proxy-Verbindung Anwendungsinformationen mit einem aEMT im WAN austauschen kann.

Diese KS besteht aus folgenden Protokollen:

- Verbindungsorientiertes Transportprotokoll TCP/IP mit abgehenden Verbindungen, um eine zuverlässige Übertragung zu gewährleisten.
- TLS für das SMGW in der Rolle des Clients, um vertrauliche und authentische Transportverbindungen zwischen SMGW und einem Kommunikationspartner zu gewährleisten.
- Anwendungsnachrichten eines Anwendungsprotokolls, an die keine Interoperabilitätsanforderungen gestellt werden.

Das SMGW nimmt keine eingehenden Verbindungen an der WAN-Schnittstelle an. Stattdessen baut das SMGW eine Transport-Verbindung zum aEMT auf und führt den TLS-Handshake in der Rolle des TLS-Client aus.

▸Abbildung 4.8 verdeutlicht den Ablauf der im WKS.TLSPROXY verwendeten Kommunikationsdienste TLS-Verbindungsaufbau durch das SMGW, Transparenter Datenaustausch, und TLS-Verbindungsabbau.

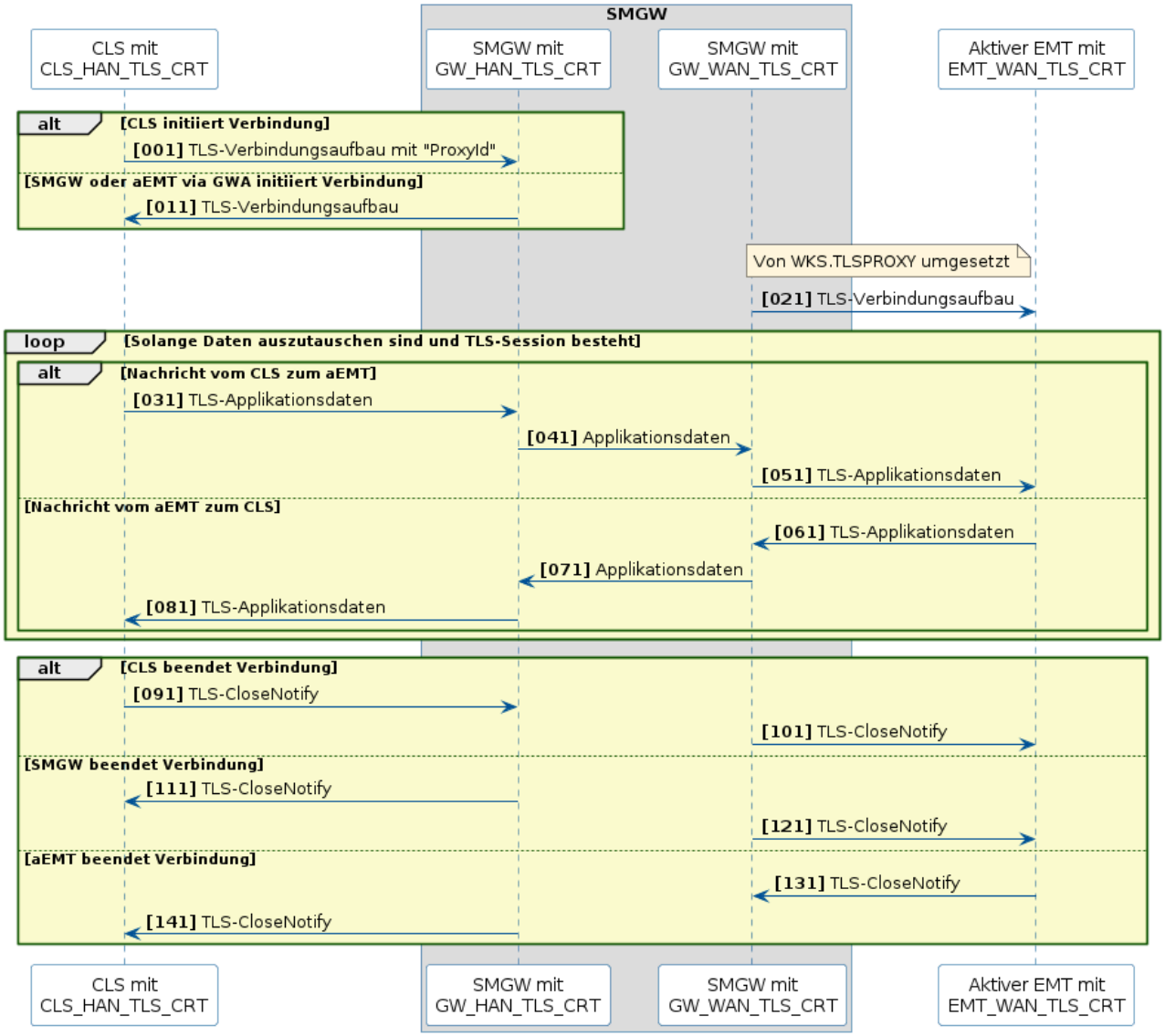


Abbildung 4.8. Übersicht über den Ablauf des WKS.TLSPROXY

4.2.11.2 Vorbedingungen

Der aktive EMT ist für das SMGW kommunikativ erreichbar.

Die Kommunikationsadresse und das den aktiven EMT identifizierende EMT-TLS-Server-Zertifikat EMT_WAN_TLS_CRT sind über ein WAN-Kommunikationsprofil im SMGW parametriert worden.

4.2.11.3 Anforderungen an die Kommunikationsprotokolle

Das Kommunikationsszenario WKS.TLSPROXY verwendet die in ▸Tabelle 4.6 beschriebenen technischen Anwendungsfälle der Kommunikationsprotokolle mit den über ein WAN-Kommunikationsprofil vom Typ ▸WKS.TLSPROXY definierten Parametern.

Das WAN-Kommunikationsprofil in der folgenden Tabelle ist immer das über ▸wanPeerRef referenzierte WAN-Kommunikationsprofil des auslösenden Proxy-Kommunikationsprofils. Beim Anlegen des WAN-Kommunikationsprofils wird gewährleistet, dass es vom Typ ▸WKS.TLSPROXY ist.

Aufgabe	Detailspezifikation	Parameter
Aktives Öffnen einer Transport-Verbindung (abgehende Verbindung)	TCP gemäß [RFC9293]	Das SMGW **MUSS** eine TCP-Verbindung gemäß [RFC9293] in der Rolle des Initiators (Active Opener) zur ersten der in ▸outboundConnection.addresses angegebenen Transport-Adressen über die Schnittstelle gemäß ▸outboundConnection.ifName initiieren. [REQ.WKS.TLS-PROXY.10]

Aufgabe	Detailspezifikation	Parameter
Öffnen einer TLS-Session als Client	[DS] Kapitel "TLS" TA.TLS.OpenWanSessionAsClient, TA.TLS.Handshake	Anforderungen an die TLS-Authentifizierung zwischen SMGW und EMT-Kommunikationssystem sind in ▸Abschnitt 4.2.4 beschrieben. Das SMGW **MUSS** TLS gemäß [DS] Kapitel TLS in der Rolle des Clients verwenden. [REQ.WKS.TLS-PROXY.20] Das SMGW **MUSS** die TLS-Verbindung zum EMT mit den Parametern des WAN-Kommunikationsprofils aufbauen. [REQ.WKS.TLS-PROXY.30] Das SMGW **MUSS** das ▸peerCerts.tlsCert aus dem WAN-Kommunikationsprofil verwenden, um den TLS-Server des EMT zu authentifizieren. [REQ.HAN.HKS4.50]
Schließen der TCP/TLS-Verbindung nach Empfang eines Close-Notify Alerts	[DS] Kapitel "TLS" TA.TLS.Close	Siehe ▸REQ.WAN.Transport.80 Das SMGW **MUSS** die TLS-Verbindung des zugeordneten WAN-Kommunikationsprofils beenden, falls ▸outboundConnection.idleTimeout > 0 und mehr als ▸outboundConnection.idleTimeout Sekunden ohne TLS-Applikationsdatentransfer vergangen sind. [REQ.WKS.TLS-PROXY.40]
Schließen der TCP/TLS-Verbindung, initiiert durch das SMGW		

Tabelle 4.6 Anforderungen an die Protokolllayer des WKS.TLSPROXY

4.2.12 Kommunikationsszenario WKS.WAKEUP: Wake-Up Dienst des SMGW

4.2.12.1 Beschreibung

Das WKS.WAKEUP fasst die Protokolle und Nachrichtenformate zusammen, über die der GWA eine Management-Verbindung vom SMGW anfordern kann.

Das Wake-Up-Protokoll besteht aus einer (unbestätigten) Nachricht, die vom GWA an das SMGW gesendet wird. Das SMGW antwortet nach erfolgreicher Prüfung der Nachricht mit einem TLS-Verbindungsaufbau WKS.MANAGEMENT an den GWA.

Es existieren keine Anforderungen an den Transportweg der Wake-Up-Nachricht. Die Nachricht wird über eine WAN-Schnittstelle des SMGW empfangen. Diese WAN-Schnittstelle ist nicht zwangsläufig identisch mit der WAN-Schnittstelle, über die anschließend auch die TLS-Verbindung aufgebaut wird.

Dieses KS referenziert folgende Protokolle:

- Verbindungsloses oder verbindungsorientiertes Transportprotokoll, über welches das SMGW die kurze, binär-codierte Wake-Up-Nachricht empfängt. Das Transportprotokoll UDP/IP ist mindestens zu unterstützen.
- Wake-Up-Protokoll, wobei das SMGW Message-Recipient ist.

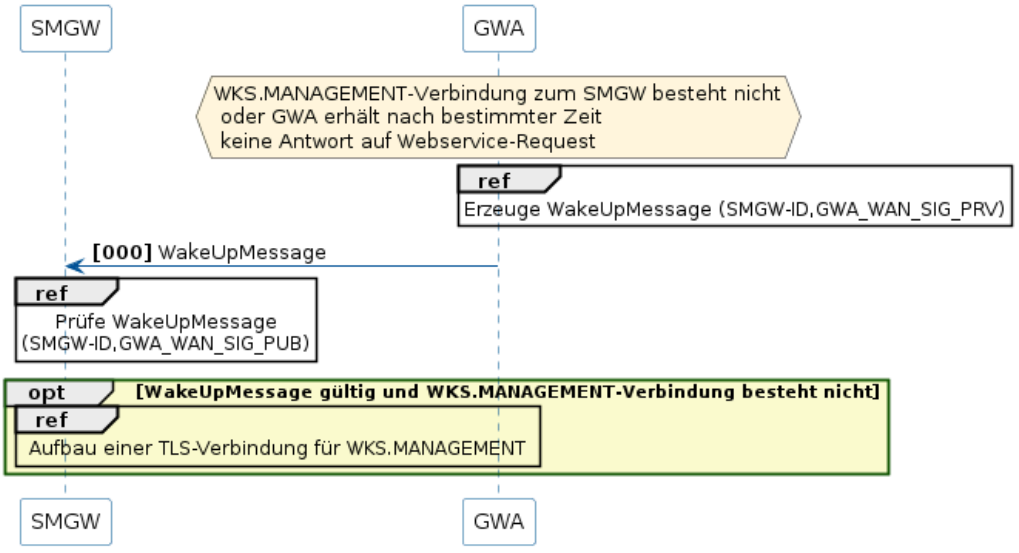


Abbildung 4.9. Übersicht der Interaktion zwischen WKS.WAKEUP und WKS.MANAGEMENT

4.2.12.2 Vorbedingungen

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

Der zur Signaturprüfung der Wake-Up-Nachricht verwendete Schlüssel (GWA_WAN_SIG_PUB aus dem Zertifikat GWA_WAN_SIG_CRT) ist durch den GWA oder bei der Vorpersonalisierung im SMGW parametriert worden.

4.2.12.3 Sicherung der Kommunikation

Um das SMGW vor Angriffen aus dem WAN auf den Wake-Up-Dienst zu schützen, müssen Nachrichten verworfen (ignoriert) werden, die den folgenden Anforderungen nicht genügen. Insbesondere werden im Fehlerfall keine Nachrichten an den Absender gesendet, um keine Reflection/Amplification-Angriffe zu ermöglichen.

a. Das SMGW **MUSS** Wake-Up Nachrichten ignorieren, wenn Nachrichtenlänge oder Datenfeldinhalte nicht den Vorgaben der [DS] "Wake-Up Nachricht" entsprechen. [REQ.WAN.WakeUpSicherung.10]

b. Das SMGW **MUSS** Wake-Up Nachrichten ignorieren, bei denen die Identifikation des Empfängers der Wake-Up Nachricht nicht mit der HÜID des SMGW (gemäß *SubjectCN* der SM-PKI-Zertifikate des SMGW) übereinstimmt. [REQ.WAN.WakeUpSicherung.20]

c. Das SMGW **MUSS** Wake-Up Nachrichten ignorieren, die innerhalb kurzer Zeit (30s) identisch empfangen wurden. [REQ.WAN.WakeUpSicherung.30]

d. Sofern die Systemzeit des SMGW mit dem Zeitserver des GWA synchronisiert ist und der Zeitstempel der Wake-Up Nachricht, um mehr als +/-30s von der Systemzeit abweicht **MUSS** das SMGW die Wake-Up Nachricht ignorieren. [REQ.WAN.WakeUpSicherung.40] Dies soll das Wiederverwenden des Paketes zu einem späteren Zeitpunkt verhindern.

e. Das SMGW **MUSS** Wake-Up Nachrichten ignorieren, die nicht mit dem öffentlichen Schlüssel aus dem im SMGW konfigurierten $GWA_WAN_SIG_CRT_n$ oder $GWA_WAN_SIG_CRT_{n+1}$ validiert werden können. [REQ.WAN.WakeUpSicherung.50]

f. Das SMGW **SOLL** Wake-Up Nachrichten für 1 Minute ignorieren, sofern mehr als 10 valide Wake-Up Nachrichten innerhalb einer Minute empfangen werden (Siehe ▸ICS.WAN.WakeUpSicherung.10). ▸ [FNN.7001.6] [REQ.WAN.WakeUpSicherung.60] Damit sollen Angriffe auf die Leistungsfähigkeit des SMGW vermieden werden.

g. Das SMGW **MUSS** Wake-Up Nachrichten ignorieren, deren Signatur gemäß REQ.WAN.WakeUpSicherung.50 validiert wurde, die innerhalb des Zeitfensters REQ.WAN.WakeUpSicherung.40 eintreffen, aber eine Wiederholung (Replay) einer bereits verarbeiteten Wake-Up-Nachricht sind. ▸ [BSI.7001.7] [REQ.WAN.WakeUpSicherung.80] Damit sollen Angriffe auf die Leistungsfähigkeit des SMGW vermieden werden.

4.2.12.4 Anforderungen an die Kommunikationsprotokolle

Das Kommunikationsszenario WKS.WAKEUP verwendet die in ▸Tabelle 4.7 beschriebenen technischen Anwendungsfälle der Kommunikationsprotokolle mit den über das WAN-Schnittstellenprofil definierten Parametern.

Aufgabe	Detailspezifikation	Parameter
Verbindungsloser Nachrichtenempfang	UDP gemäß [RFC768]	Das SMGW **MUSS** eine Wake-Up-Nachricht über die vereinbarte Portnummer empfangen können. [REQ.WKS.WAKEUP.10] Die Portnummer wird durch den GWH bei der Bestellung festgelegt. Das SMGW **MUSS** Wake-Up Nachrichten auf der Schnittstelle unter der IP-Adresse empfangen, die als Quelladresse abgehender Verbindungen für WKS.MANAGEMENT verwendet wird. [REQ.WKS.WAKEUP.30]

Aufgabe	Detailspezifikation	Parameter
Verarbeiten einer Wake-Up-Nachricht	[DS] Kapitel "Wake-Up-Nachricht"	Es gelten die Anforderungen zur Sicherung der Wake-Up-Kommunikation in ▸Abschnitt 4.2.12.3. Das SMGW **MUSS** die Wake-Up-Nachricht gemäß [DS] Kapitel "Wake-Up-Nachricht" Version 1 zu dieser Technischen Richtlinie verarbeiten. [REQ.WAN.WAKEUP.20]

Tabelle 4.7 Anforderungen an die Protokolllayer des WKS.WAKEUP

ICS



ICS.WAN.WakeUpSicherung.10

Der GWH **MUSS** im ICS deklarieren, ob das SMGW die Rate der verarbeiteten Wake-Up Nachrichten begrenzt.

4.2.12.5 Implementierungshinweise

Um ein Verdrängen von Syslog-Einträgen aus dem Ringspeicher zu vermeiden, sollte die Protokollierung von Ereignissen nicht authentifizierter Wake-Up Nachrichten innerhalb eines kurzen Zeitraumes begrenzt werden.

4.2.13 Kommunikationsszenario WKS.DOWNLOAD: Download vom GWA mit dem SMGW als Client

4.2.13.1 Beschreibung

Das WKS.DOWNLOAD fasst die Protokolle und Nachrichtenformate für den Download von (Firmware-)Dateien mittels HTTPS vom Fileserver des GWA zusammen.

Dieses KS besteht aus folgenden Protokollen:

- Verbindungsorientiertes Transportprotokoll TCP mit vom SMGW abgehenden Verbindungen.
- TLS in der Rolle des Clients, um vertrauliche und authentische Transportverbindungen zwischen SMGW und einem Kommunikationspartner zu gewährleisten.
- HTTP in der Rolle des Clients, um die Dateien mittels Webservice von einem Fileserver auszulesen.

Das SMGW nutzt den Fileserver des GWA zum Download der Firmware-Dateien mittels HTTPS-Protokoll.

▸Abbildung 4.10 verdeutlicht den Ablauf, der im WKS.DOWNLOAD verwendeten Kommunikationsdienste TLS-Verbindungsaufbau, TLS-Verbindungsabbau und Firmware-Download.

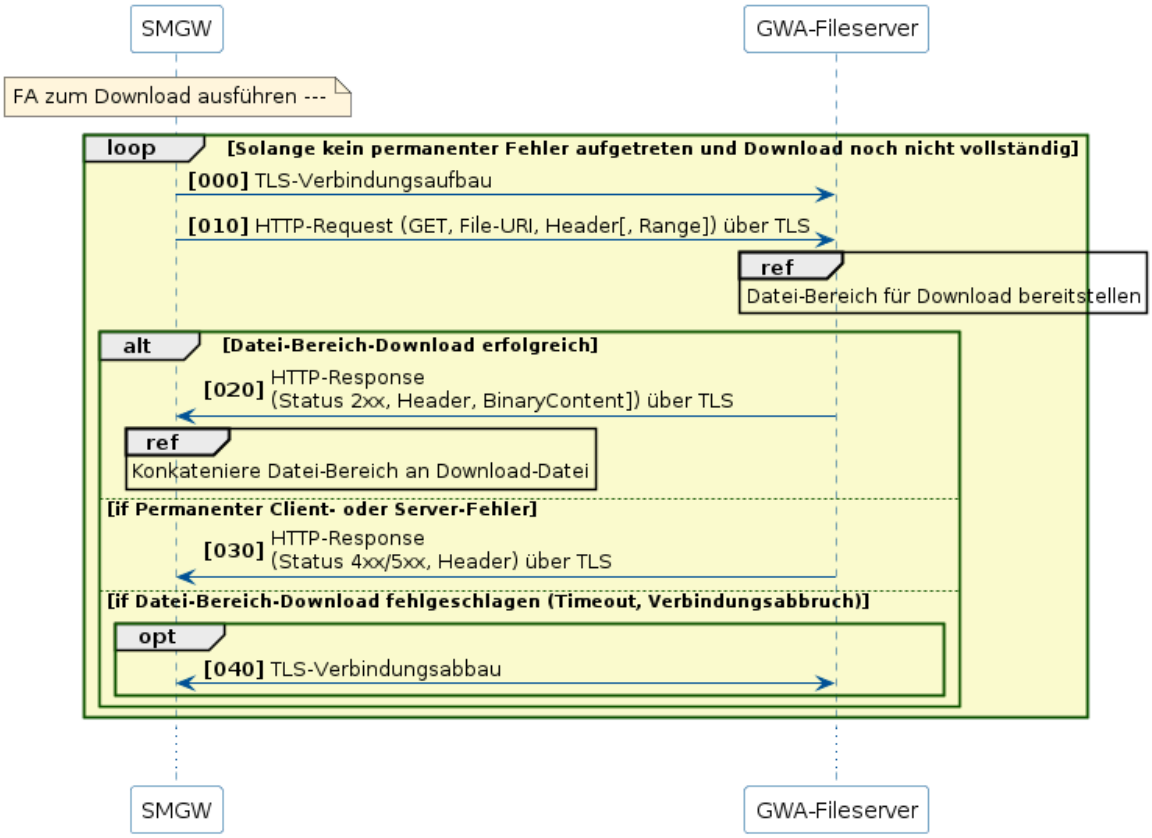


Abbildung 4.10. Übersicht über den Ablauf des WKS.DOWNLOAD

4.2.13.2 Vorbedingungen

Die Kommunikationsparameter des GWA-Fileservers sind im SMGW konfiguriert (Siehe ▸Abschnitt 3.22.46).

Die Kommunikationsadresse und das den GWA identifizierende TLS-Server-Zertifikat GWA_WAN_TLS_CRT sind durch den GWA oder bei der Vorpersonalisierung über ein WAN-Kommunikationsprofil im SMGW konfiguriert worden.

Der Fileserver des GWA ist über eine TCP/IP-Verbindung zur konfigurierten Kommunikationsadresse kommunikativ erreichbar.

4.2.13.3 Anforderungen an die Kommunikationsprotokolle

Das Kommunikationsszenario WKS.DOWNLOAD verwendet die in ▸Tabelle 4.8 beschriebenen technische Anwendungsfälle der Kommunikationsprotokolle mit den über ein WAN-Kommunikationsprofil vom Typ "DOWNLOAD" definierten Parametern.

Aufgabe	Detailspezifikation	Parameter
Aktives Öffnen einer Transport-Verbindung (abgehende Verbindung)	TCP gemäß [RFC9293]	Das SMGW **MUSS** eine TCP-Verbindung gemäß [RFC9293] in der Rolle des Initiators (Active Opener) zur ersten der in ▸outboundConnection.addresses angegebenen Transport-Adressen über die Schnittstelle gemäß ▸outboundConnection.ifName initiieren. [REQ.WKS.DOWNLOAD.10]
Öffnen einer TLS-Session als Client	[DS] Kapitel "TLS" TA.TLS.OpenWanSessionAsClient, TA.TLS.Handshake	Anforderungen an die TLS-Authentifizierung zwischen SMGW und GWA-Kommunikationssystem sind in ▸Abschnitt 4.2.4 beschrieben. Das SMGW **MUSS** TLS gemäß [DS] Kapitel TLS in der Rolle des Clients verwenden. [REQ.WKS.DOWNLOAD.20] Das SMGW **MUSS** die TLS-Verbindung zum GWA mit den Parametern des WAN-Kommunikationsprofiles der Domäne "gwa-download" aufbauen. ▸ [BSI.9007.0] ▸ [BSI.9007.1] [REQ.WKS.DOWNLOAD.50]

Aufgabe	Detailspezifikation	Parameter
Schließen der TCP/ TLS-Verbindung nach Empfang eines Close-Notify Alerts	[DS] Kapitel "TLS" TA.TLS.Close	Siehe ▸REQ.WAN.Transport.80
Schließen der TCP/ TLS-Verbindung, initiiert durch das SMGW		
Senden einer HTTP-Anfrage	[DS] Kapitel "RESTful Webservice" Anforderungen an HTTP-Clients	Das SMGW **MUSS** HTTP gemäß [DS] Kapitel RESTful Webservice in der Rolle des Clients verwenden. [REQ.WKS.DOWNLOAD.30] Das SMGW **MUSS** Nachrichten über WKS.DOWNLOAD an den GWA mittels HTTP "GET"-Request an die URI ▸downloadUri des auslösenden FirmwareUpdateProfils senden. [REQ.WKS.DOWNLOAD.60] Das SMGW **MUSS** für den Datei-Download eine HTTP-Abfrage mit Range-Requests verwenden. [REQ.WKS.DOWNLOAD.40]
Verarbeiten einer HTTP-Antwort	[DS] Kapitel "RESTful Webservice" Anforderungen an HTTP-Clients	Das SMGW **MUSS** bis zu ▸outboundConnection.serviceTimeout Sekunden auf eine HTTP-Antwort warten ▸ [BSI.2003.1] . [REQ.WKS.DOWNLOAD.80] Das SMGW **MUSS** den Statuscode der HTTP-Response protokollieren. ▸ [BSI.2003.2] ▸ [BSI.2003.0] [REQ.WKS.DOWNLOAD.100]

Tabelle 4.8 Anforderungen an die Protokolllayer des WKS.DOWNLOAD

4.2.13.4 Implementierungshinweise

Der Inhalt des Datenfeldes ▸messageFormat soll nicht vorhanden sein bzw. wird nicht berücksichtigt.

4.3 Kommunikation des SMGW im LMN

4.3.1 Einleitung

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 beschrieben und können in folgende Kategorien eingeteilt werden:

1. kommunikative Anbindung von Messeinrichtungen (bisher LAF1)
2. Anfordern und Empfang von Messwerten (bisher LAF2)

Die zur Realisierung dieser Anwendungsfälle notwendigen Kommunikationsszenarien werden in ▸Abschnitt 4.3.2 definiert.

Die Anforderungen an die Sicherung der Kommunikation im LMN werden in ▸Abschnitt 4.3.4 beschrieben.

Die Festlegungen zu den Kommunikationsprotokollen, die für drahtgebundene und drahtlose Zähler vom SMGW mindestens unterstützt werden müssen, folgen in ▸Abschnitt 4.3.3.

4.3.2 LMN-Kommunikationsszenarien

- 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

Szenario	Typ	Service Requester	Service Provider
LKS2	UNIDIREKTIONAL	-	Zähler

Tabelle 4.9 Kommunikationsszenarien an der LMN-Schnittstelle

4.3.3 LMN-Kommunikationsprotokolle

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

Die ▸Abbildung 4.11 zeigt die Gesamtheit der LMN-Protokollstapel im SMGW. Die Protokollstapel haben abhängig von der physikalischen Schicht unterschiedliche Ausprägungen, die in den nächsten Abschnitten detailliert werden.

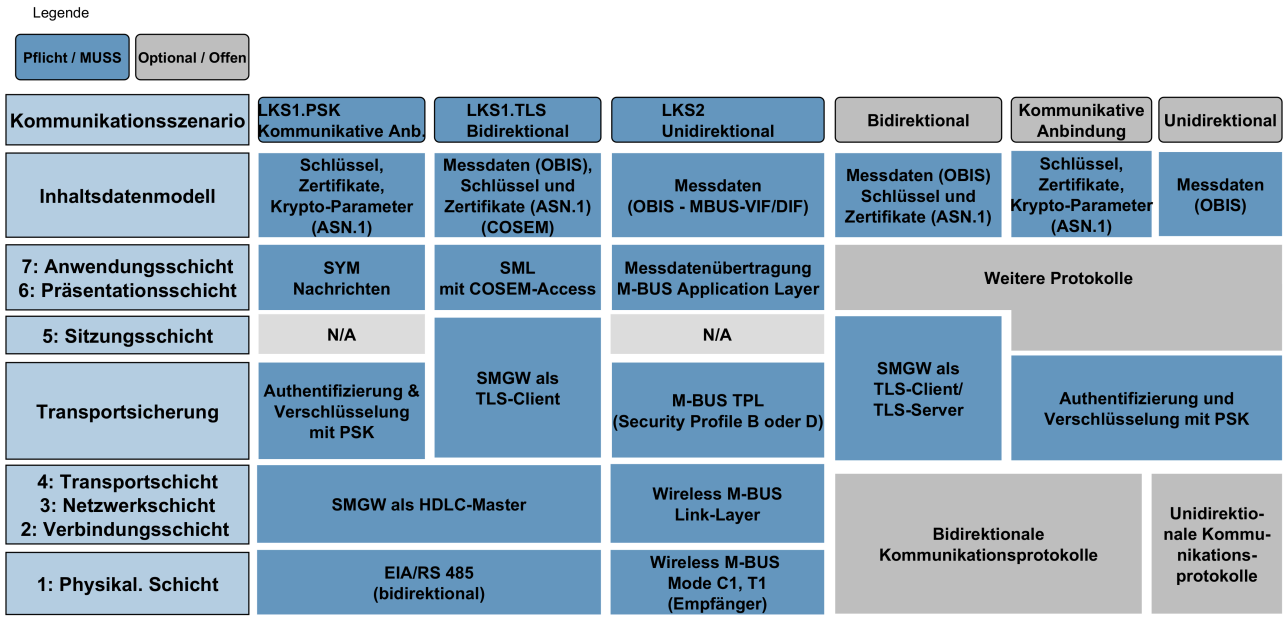


Abbildung 4.11. Protokollstapel im LMN (für drahtlose und drahtgebundene Kommunikation)

Anwendungsprotokolle

Das SMGW **MUSS** die Anwendungsprotokoll-spezifische Codierung der Maßeinheiten und die Identifikation der *Messgrößen* und *Messarten* für elektrische Energie nach [EN62056-6-1] und andere Sparten nach [EN13757-1] mindestens für die in den Anwendungsfällen der Messwertverarbeitung (Siehe ▸Kapitel 3) verwendeten Messgrößen und Messarten umsetzen. [REQ.LMN.Anwendungsprotokolle.10] [2]

Das SMGW **MUSS** die Anwendungsprotokoll-spezifische Identifikation der Messeinrichtung in die Identifikation nach [DIN43849] umsetzen. [REQ.LMN.Anwendungsprotokolle.20]

Das SMGW **MUSS** die Anwendungsprotokoll-spezifische Codierung von Fehlern (bspw. Integritätsverletzung an der Messeinrichtung, ungültiger Messwert oder zu geringe Versorgungsspannung) der Messwertverarbeitung des SMGW mitteilen. [REQ.LMN.Anwendungsprotokolle.30]

4.3.4 Sicherung der Kommunikationsverbindungen in das LMN

Das SMGW **MUSS** sicherstellen, dass Messwerte, die von Zählern empfangen werden, nur dann akzeptiert werden, wenn sie über eine gesicherte Kommunikation vertraulich, integer und authentisch empfangen wurden. [REQ.LMN.Sicherung.10] Das SMGW gewährleistet diese Anforderung über die in den folgenden Ab-

[2] Die für die Messwertverarbeitung im SMGW zulässigen OBIS-Kennzahlen werden über das Regelwerk der Tarifanwendungsfälle bestimmt.

schnitten beschriebene Sicherung der Kommunikation, die sich für bidirektional und unidirektional kommunizierende Zähler unterscheidet.

4.3.5 LMN-Netzwerk-Schnittstellen

Das SMGW **MUSS** im LMN eine drahtlose physische Schnittstelle für den Empfang von Messwerten über LKS2 besitzen. [REQ.LMN.Kommunikationsprotokolle.10]

Das SMGW **MUSS** im LMN eine physische Schnittstelle für den Abruf von Messwerten über LKS1 besitzen. [REQ.LMN.Kommunikationsprotokolle.11]

ICS



ICS.LMN.Sicherung.10

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

4.3.6 Kommunikationsszenario LKS1: Bidirektionale leitungsgebundene LMN Kommunikation

4.3.6.1 Beschreibung des Protokollstacks

Dieses Kommunikationsszenario fasst die Protokolle und Nachrichtenformate für eine interoperable, bidirektionale, leitungsgebundene Messwertübermittlung und die Aufrechterhaltung einer sicheren Kommunikation zwischen einer Messeinrichtung und dem SMGW über die LMN-Schnittstelle zusammen.

Dieses KS besteht aus folgenden Protokollen:

- Leitungsgebundene, asynchrone, serielle, Halb-Duplex-Kommunikation nach EIA/RS-485 zwischen Messeinrichtung und SMGW.
- Verbindungsorientiertes Transportprotokoll mit dem SMGW als primäre Kommunikationsstation um eine zuverlässige Übertragung zu gewährleisten.
- TLS in der Rolle des Clients, um vertrauliche und authentische Transportverbindungen zwischen SMGW und einem Kommunikationspartner zu gewährleisten. Dabei werden auf dem Transportweg vertauschte oder wiederholte Nachrichten erkannt und verworfen.
- Applikationsprotokoll SML in der Rolle des Clients, um die Messwerte und den Status der Messeinrichtung abzufragen, entgegenzunehmen und die Messeinrichtung zu konfigurieren.
- Datenmodell COSEM und Identifikation der Messgrößen gemäß OBIS

Diese Protokolle sind in ▸Abbildung 4.12 dargestellt.

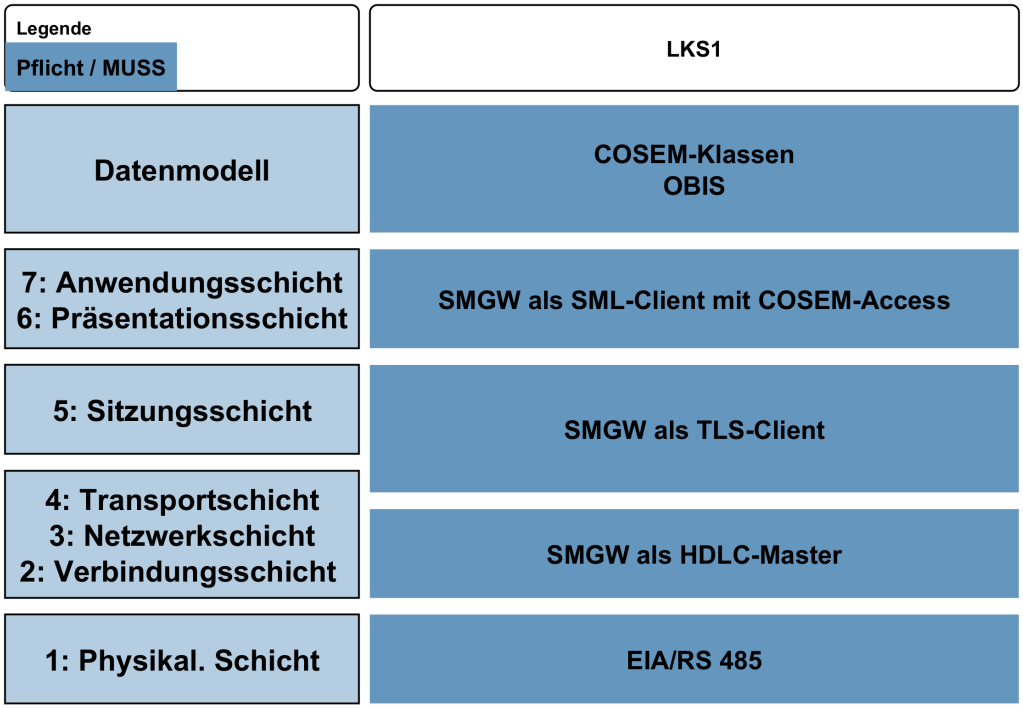


Abbildung 4.12. Übersicht über den Protokollstapel von LKS1

Abbildung 4.13 verdeutlicht den Ablauf der im LKS1 verwendeten Kommunikationsdienste HDLC-Verbindungsaufbau, TLS-Verbindungsaufbau, SML-Anfrage an die Messeinrichtung und SML-Antwort.

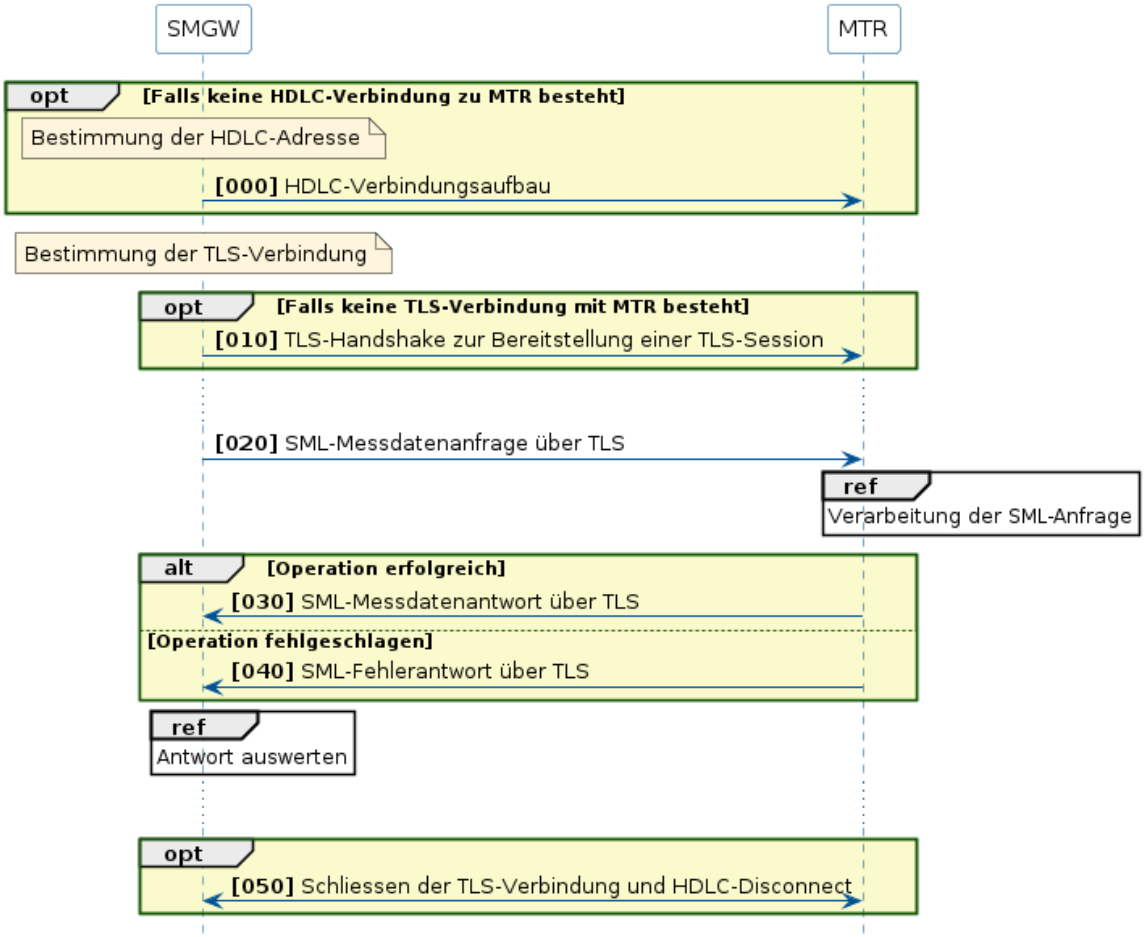


Abbildung 4.13. Übersicht über den Ablauf des LKS1.TLS

4.3.6.2 Vorbedingungen

Vorbedingung für die Kommunikation des SMGW mit der Messeinrichtung als LMN-Teilnehmer ist die erfolgreiche kommunikative Anbindung:

- Die Berechtigung zur Kommunikation mit dem SMGW über ein vom GWA konfiguriertes LMN-Kommunikationsprofil (Zählerprofil) liegt im SMGW vor.
- Die Schlüssel und Zertifikate zur TLS-Kommunikation wurden zwischen SMGW und Zähler vereinbart.
- Die Zuordnung einer HDLC-Adresse zur Zähler-ID der Messeinrichtung ist im SMGW erfolgt

4.3.6.3 Anforderungen an die Kommunikationsprotokolle

Das Kommunikationsszenario LKS1 verwendet die in ▸Tabelle 4.10 beschriebenen technischen Anwendungsfälle der Kommunikationsprotokolle mit den über ein LMN-Kommunikationsprofil vom Typ ▸ks gleich "LKS1" und der ▸meterId definierten Parametern.

Aufgabe	Detailspezifikation	Anforderungen
Bestimmung der HDLC-Adresse der Messeinrichtung zur meterId	[DS] Kapitel "LMN HDLC Protokoll"	Sofern die HDLC-Kommunikationsadresse der Messeinrichtung nicht durch ▸address konfiguriert ist, **MUSS** das SMGW die HDLC-Adresse der Messeinrichtung aus der ▸meterId gemäß [DS] bestimmen. ▸ [BSI.1001.1] [REQ.LMN.LKS1.10]
Aufbau einer HDLC-Verbindung zur Messeinrichtung	[DS] Kapitel "LMN HDLC Protokoll"	Das SMGW **MUSS** die bidirektionale, drahtgebundene Kommunikation im LMN (LKS1) mit einem Protokollstapel TLS - HDLC - RS485 gemäß der Anforderungen [DS] Kapitel "LMN HDLC Protokoll" unterstützen. [REQ.LMN.Kommunikationsprotokolle.40]
Öffnen einer TLS-Session als Client	[DS] Kapitel "TLS" TA.TLS.OpenLmnSessionAsClient, TA.TLS.Handshake	Das SMGW **MUSS** TLS gemäß [DS] Kapitel TLS in der Rolle des Clients verwenden. [REQ.LMN.Kommunikationsprotokolle.42] Das SMGW **MUSS** die HDLC/TLS-Verbindung mit TLS-Alert beenden, sofern das empfangene TLS-Client-Zertifikat nicht dem ▸mtrTlsCert entspricht. ▸ [FNN.1004.0] ▸ [FNN.1004.1] [REQ.LMN.LKS1.30] Das SMGW **MUSS** sich mit dem GW_LMN_TLS_CRT ▸smgwTlsCert gemäß [DS] Kapitel "LMN Zertifikatsprofile" als TLS-Client authentisieren. [REQ.LMN.LKS1.20] Das SMGW **MUSS** die TLS-Verbindung nach Beendigung der auslösenden Aktion geöffnet lassen. [REQ.LMN.LKS1.40]
Schließen der HDLC/TLS-Verbindung nach Empfang eines Close-Notify Alerts	[DS] Kapitel "TLS" TA.TLS.Close	
Schließen der HDLC/TLS-Verbindung, initiiert durch das SMGW		Das SMGW **MUSS** die TLS-Sitzungsschlüssel beim Erreichen der maximalen Sitzungsdauer gemäß [TR-03109-3] erneuern und die TLS-Verbindung beenden, sofern eine Erneuerung (TLS1.3) nicht möglich ist. [REQ.LMN.LKS1.50]
Erstellen einer Messwertabfrage	[DS] Kapitel "SML - Smart Message Language"	Das SMGW **MUSS** die Messwertabfrage gemäß [DS] Kapitel "SML - Smart Message Language" erstellen. [REQ.LMN.Kommunikationsprotokolle.51]
Empfangen einer Messwertnachricht		Das SMGW **MUSS** die Messwerte und Statusinformationen der Anwendungsschicht gemäß [DS] Kapitel "SML - Smart Message Language" verarbeiten und die *Messgrößen* und *Messarten* nach OBIS-Kennzahlen gemäß [EN13757-1] und [EN62056-6-1] identifizieren. ▸ [BSI.1009.1] ▸ [BSI.1006.1] ▸ [FNN.1014.1] [REQ.LMN.Kommunikationsprotokolle.50]
Lesen von Geräteinformationen	[DS] Kapitel "SML - Smart Message Language"	Siehe Detailspezifikation.
Verändern/Schreiben eines Konfigurationsregisters	[DS] Kapitel "SML - Smart Message Language"	Siehe Detailspezifikation.

Aufgabe	Detailspezifikation	Anforderungen
Dateitransfer vom SMGW zum Zähler	[DS] Kapitel "SML - Smart Message Language"	Abhängig von ▸ICS.FAKAT.ValProcBilling.20 (Unterstützung RLM-Messeinrichtung): Siehe Detailspezifikation.
Dateitransfer vom Zähler zum SMGW	[DS] Kapitel "SML - Smart Message Language"	Abhängig von ▸ICS.FAKAT.ValProcBilling.20 (Unterstützung RLM-Messeinrichtung): Siehe Detailspezifikation.
Übermitteln der Zeit vom SMGW an die Messeinrichtung	[DS] Kapitel "SML - Smart Message Language"	Abhängig von ▸ICS.FAKAT.ValProcBilling.20 (Unterstützung RLM-Messeinrichtung): Siehe Detailspezifikation.
Übermitteln des Uhrenzustandes der Messeinrichtung an das SMGW	[DS] Kapitel "SML - Smart Message Language"	Abhängig von ▸ICS.FAKAT.ValProcBilling.20 (Unterstützung RLM-Messeinrichtung): Siehe Detailspezifikation.

Tabelle 4.10 Übersicht der TA des LKS1

4.3.6.4 Implementierungshinweise

Um Verzögerungen der Übermittlung von Messwertabfragen an die Messeinrichtung zu vermeiden, wird empfohlen die TLS-Verbindung den TLS-Verbindungsaufbau rechtzeitig vor der Messwertabfrage zu initiieren, da der vollständige TLS-Handshake (ohne Verkürzung durch Session-Resumption) mit Messeinrichtungen einige Sekunden in Anspruch nehmen kann.

Es wird empfohlen TLS1.3 für künftige Implementierungen vorzusehen (siehe [DS] Kapitel "TLS"). Das TLS-1.3-Protokoll lässt eine Erneuerung der Sitzungsschlüssel bei bestehender Verbindung zu. Ein Verbindungsabbau/Aufbau ist zur Erneuerung der Sitzungsschlüssel nicht notwendig.

4.3.7 Kommunikationsszenario LKS1.PSK: kommunikative Anbindung bidirektional kommunizierender Messeinrichtungen

4.3.7.1 Beschreibung

Dieses Kommunikationsszenario fasst die Protokolle und Nachrichtenformate für eine sichere Kommunikative Anbindung einer bidirektional kommunizierenden Messeinrichtung im LMN an ein SMGW auf Basis eines gemeinsamen, geräteindividuellen geheimen Schlüssels (Pre-Shared Key, PSK) zusammen. Nach kommunikativer Anbindung kommunizieren SMGW und Messeinrichtung über LKS1 mit TLS mit beidseitiger, zertifikatsbasierter Authentifizierung.

Dieses KS besteht aus folgenden Protokollen:

- Leitungsgebundene, asynchrone, serielle, Halb-Duplex-Kommunikation nach EIA/RS-485 zwischen Messeinrichtung und SMGW.
- Verbindungsorientiertes Transportprotokoll HDLC mit dem SMGW als primäre Kommunikationsstation (Master) um eine zuverlässige Übertragung zu gewährleisten.
- Authentischer und verschlüsselter Nachrichtenaustausch von Zertifikaten und Schlüsselpaaren mit symmetrischer Verschlüsselung mit SYM-Protokoll gemäß Detailspezifikation zu dieser TR.

Diese Protokolle sind in ▸Abbildung 4.14 dargestellt.

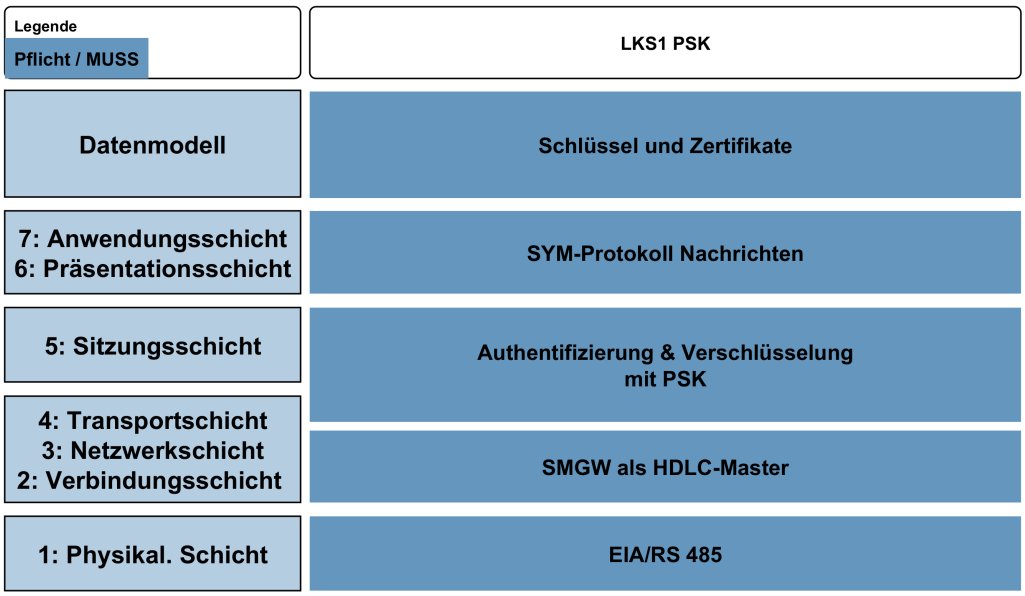


Abbildung 4.14. Übersicht über den Protokollstapel von LKS1.PSK

Abbildung 4.15 verdeutlicht den Ablauf, der im LKS1 verwendeten Kommunikationsdienste HDLC-Verbindungsaufbau, TLS-Verbindungsaufbau, SML-Anfrage an die Messeinrichtung und SML-Antwort.

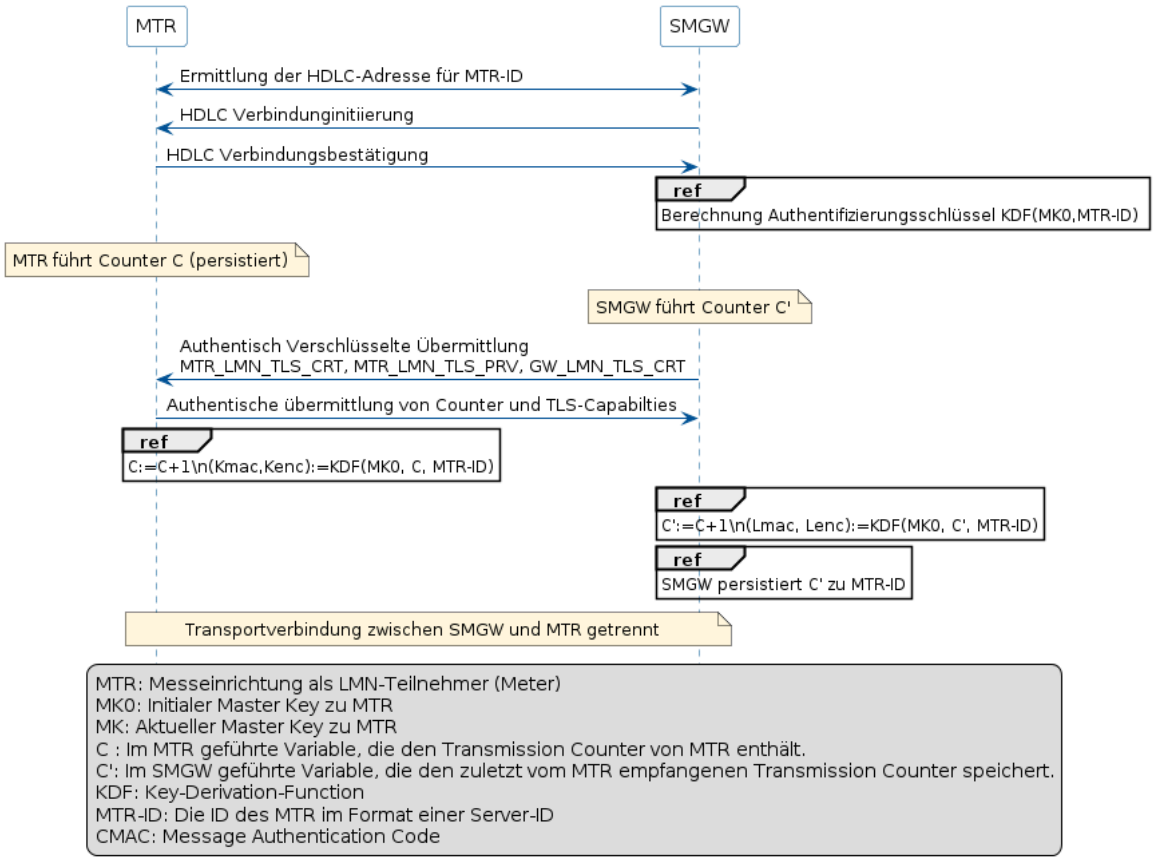


Abbildung 4.15. Übersicht über den Ablauf des LKS1.PSK

4.3.7.2 Vorbedingungen

Vorbedingung für die Kommunikation des SMGW mit der Messeinrichtung als LMN-Teilnehmer ist die erfolgreiche kommunikative Anbindung:

- Die Berechtigung zur Kommunikation mit dem SMGW über ein vom GWA konfiguriertes LMN-Kommunikationsprofil (Zählerprofil) mit dem zählerindividuellen PSK liegt im SMGW vor.

- Die Zuordnung einer HDLC-Adresse zur Zähler-ID der Messeinrichtung ist im SMGW erfolgt.

4.3.7.3 Technische Anwendungsfälle der Kommunikationsprotokolle

Das Kommunikationsszenario LKS1.PSK verwendet die in ▸Tabelle 4.11 beschriebenen technischen Anwendungsfälle der Kommunikationsprotokolle mit den Parametern, die über ein LMN-Kommunikationsprofil vom Typ ▸ks gleich "LKS1" und ▸meterId definierten sind.

Aufgabe	Detailspezifikation	Anforderungen
Bestimmung der HDLC-Adresse der Messeinrichtung zur meterId	[VDE0418-63-7], [DS] Kapitel "LMN HDLC Protokoll"	Sofern die HDLC-Kommunikationsadresse der Messeinrichtung nicht durch ▸address konfiguriert ist, **MUSS** das SMGW die HDLC-Adresse der Messeinrichtung aus der ▸meterId gemäß [DS] bestimmen. ▸ [BSI.1001.1] [REQ.LMN.LKS1.PSK.10]
Aufbau einer gesicherten Verbindung zur Messeinrichtung	[VDE0418-63-7], [DS] Kapitel "LMN HDLC Protokoll"	Das SMGW **MUSS** empfangene und gesendete SYM-Protokoll-Nachrichten für deren ▸meterId ein LMN-Kommunikationsprofil mit Datenfeld ▸pairingKey konfiguriert ist, gemäß [DS] Kapitel "LMN HDLC Protokoll" TA.SYMHDLC.SMGW.InitialPairing mit dem Schlüssel ▸pairingKey basierend auf dem Verfahren gemäß [TR-03109-3] authentifizieren und entschlüsseln. ▸ [BSI.1005.0] ▸ [FNN.1005.1] ▸ [FNN.1005.2] [REQ.LMN.LKS1.PSK.30]
Übermittlung initialer TLS-Zertifikate und kryptografischer Parameter	[VDE0418-63-7], [DS] Kapitel "LMN HDLC Protokoll"	Das SMGW **MUSS** die kommunikative Anbindung eines gemäß LKS1 kommunizierenden Zählers im LMN gemäß Detailspezifikation [DS] Kapitel "LMN HDLC Protokoll" unterstützen. [REQ.LMN.Kommunikationsprotokolle.41]

Tabelle 4.11 Übersicht der TA des LKS1.PSK

4.3.8 Kommunikationsszenario LKS2: Unidirektionale drahtlose LMN Kommunikation

4.3.8.1 Beschreibung

Dieses LKS fasst die Protokolle und Nachrichtenformate für eine unidirektionale, drahtlose Messwertübermittlung mittels Wireless M-Bus von einer Messeinrichtung über die LMN-Schnittstelle des SMGW zusammen.

Dieses KS besteht aus folgenden Protokollen:

- Physische Medienzugangsschicht für drahtlose Kommunikation nach den Anforderungen der Detailspezifikation wM-BUS zu dieser Technischen Richtlinie für das SMGW als Short Range Device Funkempfänger.
- Data Link Layer nach den Anforderungen der Detailspezifikation wM-BUS zu dieser Technischen Richtlinie für das SMGW in der Rolle des SMGW, um den Transport der Nachrichten und die Integrität der Verbindungen zu gewährleisten.
- Zusammensetzung der Nachricht aus Data Link Telegrammen (Reassemblierung), Authentifizierung und Entschlüsselung von Nachrichten nach den Anforderungen der Detailspezifikation wM-BUS zu dieser Technischen Richtlinie für das SMGW in der Rolle des Recipients. Dabei werden auf dem Transportweg vertauschte oder wiederholte Nachrichten erkannt und verworfen.
- M-Bus Applikationslayer, Abbildung in das Datenmodell des SMGW und Identifikation über OBIS nach den Anforderungen der Detailspezifikation wM-BUS zu dieser Technischen Richtlinie für das SMGW in der Rolle "Gateway".

Diese Protokolle sind in ▸Abbildung 4.16 dargestellt.

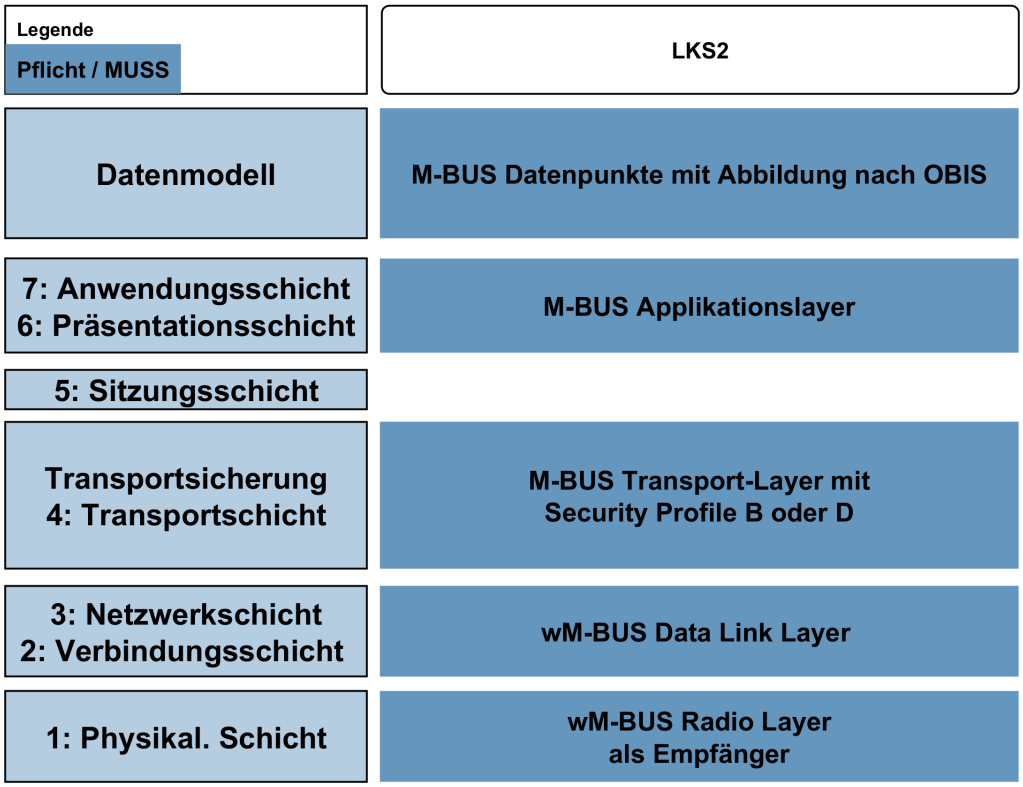


Abbildung 4.16. Übersicht über den Protokollstapel des LKS2

Das folgende Diagramm zeigt das Kommunikationsmuster bei unidirektionaler Zählerkommunikation.

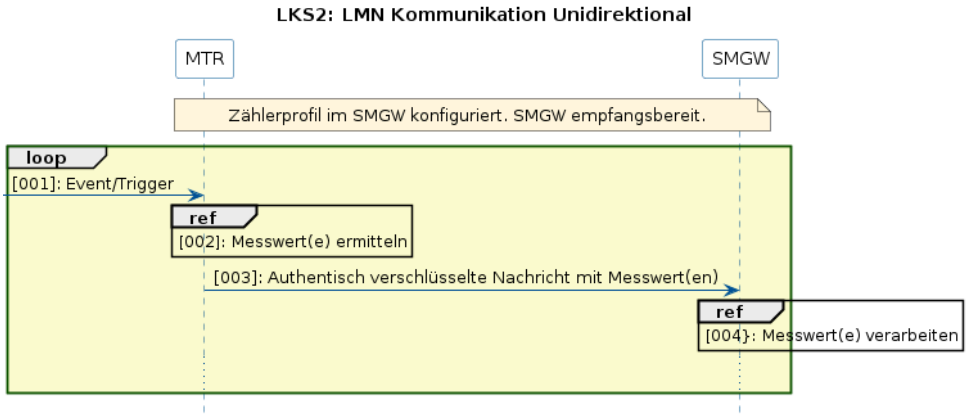


Abbildung 4.17. Sequenzdiagramm für unidirektionale LMN-Kommunikation (LKS2)

4.3.8.2 Vorbedingungen

Vorbedingung für die Kommunikation des SMGW mit der Messeinrichtung als LMN-Teilnehmer ist die erfolgreiche kommunikative Anbindung:

- Die Berechtigung zur Kommunikation mit dem SMGW über ein vom GWA konfiguriertes LMN-Kommunikationsprofil (Zählerprofil) mit dem zählerindividuellen PSK liegt im SMGW vor.
- Das SMGW ist empfangsbereit, d.h. es kann Pakete vom Zähler empfangen und entschlüsseln.

4.3.8.3 Technische Anwendungsfälle der Kommunikationsprotokolle

Das Kommunikationsszenario LKS2 verwendet die in ▸Tabelle 4.12 beschriebenen technischen Anwendungsfälle der Kommunikationsprotokolle mit den über ein LMN-Kommunikationsprofil vom Typ ▸ks gleich "LKS2" und der ▸meterId definierten Parametern.

Aufgabe	Detailspezifikation	Anforderungen
Unidirektionaler, drahtloser Empfang	[EN13757-4], [DS] Kapitel "Wireless M-Bus Protokoll"	Das SMGW **MUSS** Link-Layer-Nachrichten, die an ▸meterId - oder sofern konfiguriert ▸address - adressiert sind gemäß [EN13757-4], [DS] Kapitel "Wireless M-Bus Protokoll" auswerten. [REQ.LMN.LKS2.10]
Transportsicherung, PSK-basiert	[EN13757-7], [DS] Kapitel "Wireless M-Bus Protokoll"	Das SMGW **MUSS** empfangene Nachrichten, für deren ▸meterId kein LMN-Kommunikationsprofil konfiguriert ist ignorieren. [REQ.LMN.LKS2.20] Das SMGW **MUSS** empfangene Nachrichten, für deren ▸meterId ein LMN-Kommunikationsprofil konfiguriert ist, gemäß [DS] Kapitel "Wireless M-Bus Protokoll" mit dem Schlüssel ▸pairingKey basierend auf dem Verfahren gemäß [TR-03109-3] authentifizieren und entschlüsseln. Nicht authentifizierbare Nachrichten werden nicht verarbeitet. ▸ [BSI.1017.1] [REQ.LMN.LKS2.30] Sofern das Functional Package Multiple Grid Connection Points in [PP-0073] in Anspruch genommen wird, **MUSS** die Bitlänge des Message Authentication Codes mindestens 96 Bit betragen. [REQ.LMN.LKS2.40]
Empfangen einer Messwertnachricht	[EN13757-3], [DS] Kapitel "Wireless M-Bus Protokoll"	Das SMGW **MUSS** die unidirektionale, drahtlose Kommunikation im LMN (LKS2) mit einem Wireless M-Bus Protokollstapel gemäß [DS] Kapitel "Wireless M-Bus Protokoll" unterstützen. [REQ.LMN.Kommunikationsprotokolle.20] Das SMGW **MUSS** die Messwerte und Statusinformationen der M-Bus Anwendungsschicht nach Spezifikation [EN13757-3] verarbeiten und die *Messgrößen* und *Messarten* nach OBIS-Kennzahlen gemäß [EN13757-1], [EN62056-6-1] und [OMS-S2] Annex A identifizieren. [REQ.LMN.Kommunikationsprotokolle.30]

Tabelle 4.12 Übersicht der TA des LKS2

4.4 Kommunikation des SMGW im HAN

4.4.1 Einleitung

Das SMGW kommuniziert im HAN mit einem oder mehreren Komponenten der berechtigten Anschlussnutzer bzw. Anlagenbetreiber (Rolle CON), des berechtigten Servicetechnikers (Rolle SRV) und berechtigten lokalen steuerbaren Systemen (Rolle CLS). Die Berechtigungen werden über HAN- und Proxy-Konfigurationsprofile durch den GWA konfiguriert.

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 beschrieben. Zur Realisierung dieser Anwendungsfälle werden mehrere Kommunikationsszenarien herangezogen, welche vom SMGW unterstützt werden müssen. Diese werden in ▸Abschnitt 4.4.2 definiert. Die Anforderungen an die Sicherung der Kommunikationsverbindungen werden in ▸Abschnitt 4.4.4 formuliert. In ▸Abschnitt 4.4.3 werden die technischen Anforderungen an die HAN-Schnittstelle dargelegt, während "HAN-Kommunikationsprofile" (Siehe ▸Abschnitt 3.22.22) die notwendigen Parameter zur Kommunikation beschreibt.

Der Zugriff auf die Dienste des SMGW im HAN geschieht über eine Ethernet-Schnittstelle (HAN-CON oder HAN-CLS)[3]. Sowohl über HAN-CON als auch HAN-CLS werden die Ressourcen/Dienste für die Rollen SRV, CON und CLS angeboten. HAN-CON ist für den freien Zugang durch den Endkunden und Service-Techniker vorgesehen. HAN-CLS ist u.a. für die Kommunikation mit steuerbaren Anlagen zur netzdienlichen Steuerung vorgesehen. Um eine nicht kontrollierte Kommunikation zwischen HAN-CON und HAN-CLS zu vermeiden, sollen die IP-Adressbereiche von HAN-CON und HAN-CLS voneinander getrennt sein. Zukünftig wird eine Trennung dieser Netzwerke, mit separaten MAC-Adressen und IP-Adressen, gefordert.

[3] Die in TR-03109-1v1.1 und PP-0073v1.3 verwendeten logischen Schnittstellenbezeichner IF_GW_CON, IF_GW_CLS, IF_GW_SRV werden nicht mehr verwendet. IF_GW_SRV/CON/CLS bezeichnete eine logische Schnittstelle eines - über ein TLS-Verbindung identifizierten/authentifizierten - Service-Technikers/Consumers/CLS.

Ein direkter Zugriff auf die Dienste des SMGW aus dem Internet (z.B. über einen Kundenrouter) ist nicht vorgesehen.

Die in ▸Kapitel 3 skizzierten Anwendungsfälle lassen sich an der HAN-Schnittstelle auf folgende Kommunikationsszenarien (gekennzeichnet mit dem Kürzel HKS) abbilden.

4.4.2 HAN-Kommunikationsszenarien

- Das SMGW **MUSS** die Kommunikationsszenarien ▸HKS.WS1, ▸HKS.WS2 und ▸HKS.TLSPROXY.SOCKS umsetzen. [REQ.HAN.Kommunikationsszenarien.20]
- Das SMGW **MUSS** das Kommunikationsszenario ▸HKS.TLSPROXY.SRV umsetzen. [REQ.HAN.Kommunikationsszenarien.22]
- Das SMGW **MUSS** ▸HKS.TLSPROXY.CLI umsetzen. [REQ.HAN.Kommunikationsszenarien.30]
- Das SMGW **MUSS** ▸HKS.NTP-TLS.SRV umsetzen. [REQ.HAN.Kommunikationsszenarien.40]
- Das SMGW **MUSS** ▸HKS.DNSDISCOVERY umsetzen. [REQ.HAN.Kommunikationsszenarien.50]
- Das SMGW **MUSS** dabei gleichzeitig mindestens drei TLSPROXY-Verbindungen, mindestens zwei ▸HKS.WS1, ▸HKS.WS2 Webservice-Verbindungen und eine ▸HKS.NTP-TLS.SRV-Verbindung bedienen können. [REQ.HAN.Kommunikationsszenarien.60]
- Das SMGW **SOLL** gewährleisten, dass die Dauer vom Initiieren bis zum Abschluss eines erfolgreich authentifizierten TLS-Handshakes unter 10 Sekunden bleibt. [REQ.HAN.Kommunikationsszenarien.61]

Szenario	TLS-Client	TLS-Server	Client Authentifizierung	Server-Authentifizierung
▸HKS.WS1 (ehemals HKS1)	Endnutzer (Anschlussnutzer, Anlagenbetreiber, Letztverbraucher)	SMGW	*CON_HAN_TLS_CRT*	*GW_HAN_TLS_CRT*
▸HKS.WS1 (ehemals HKS1)	Servicetechniker	SMGW	*SRV_HAN_TLS_CRT*	*GW_HAN_TLS_CRT*
▸HKS.WS1 (ehemals HKS1)	CLS	SMGW	*CLS_HAN_TLS_CRT*	*GW_HAN_TLS_CRT*
▸HKS.WS2 (ehemals HKS2)	Endnutzer (Anschlussnutzer, Anlagenbetreiber, Letztverbraucher)	SMGW	Digest-Authentifizierung	*GW_HAN_TLS_CRT*
▸HKS.TLSPROXY.SOCKS (ehemals HKS3)	CLS	SMGW	*CLS_HAN_TLS_CRT*	*GW_HAN_TLS_CRT*
▸HKS.TLSPROXY.SRV	CLS	SMGW	*CLS_HAN_TLS_CRT*	*GW_HAN_TLS_CRT*
▸HKS.TLSPROXY.CLI (ehemals HKS4 oder HKS5)	SMGW	CLS	*GW_HAN_TLS_CRT*	*CLS_HAN_TLS_CRT*
▸HKS.NTP-TLS.SRV	CLS, CON, SRV	SMGW	Optional, *CON_HAN_TLS_CRT*, *SRV_HAN_TLS_CRT*, *CLS_HAN_TLS_CRT*	*GW_HAN_TLS_CRT*
▸HKS.DNSDISCOVERY	-	-	-	.

Tabelle 4.13 Kommunikationsszenarien an der HAN-Schnittstelle

Die HAN-Kommunikationsszenarien unterscheiden sich in der Art und Weise der Authentifizierung des Teilnehmers im HAN (Zertifikats- oder Username/Digest-basiert), den verwendeten Protokollen sowie der Initiierung der Verbindung. In allen Kommunikationsszenarien erfolgt die Kommunikation bidirektional.

4.4.3 HAN-Kommunikationsprotokolle

Die Kommunikation des SMGW über das HAN mit dem Anschlussnutzer, Servicetechniker, CLS wird über die in ▸Abbildung 4.18 dargestellten Protokollstapel durchgeführt:

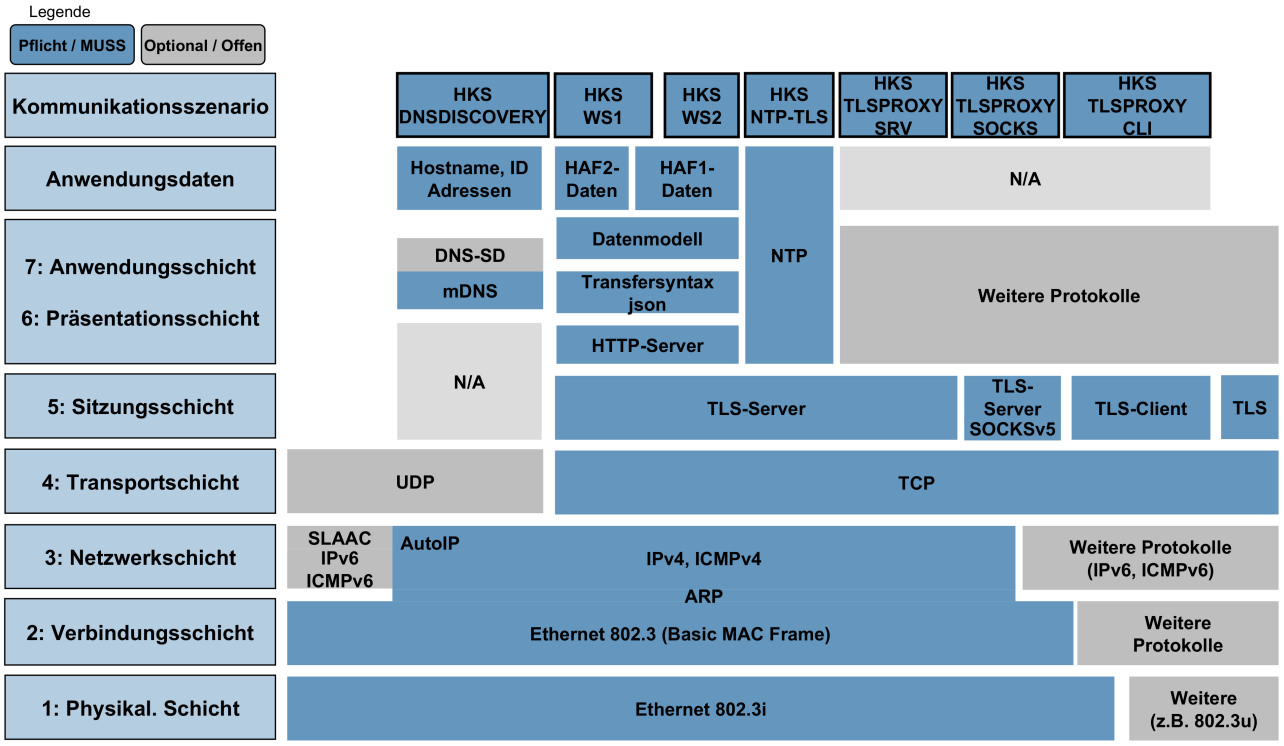


Abbildung 4.18. Protokollstapel für die HAN-Kommunikation

4.4.4 TLS-Verbindungen im HAN

Authentifizierung

Erst nach erfolgreicher zertifikatsbasierter Authentifizierung des Kommunikationspartners mittels TLS oder Username/Password-basierter Authentifizierung (HKS.WS2) erfolgt eine Zugriff auf Nutzerdaten durch das SMGW.

- Das SMGW **MUSS** sich immer mit seinem HAN-Zertifikat GW_HAN_TLS_CRT authentisieren. [REQ.HAN.SicherungKommunikation.20] GW_HAN_TLS_CRT ist gemäß [DS] Kapitel "HAN-Zertifikatsprofile" entweder vom Typ CT_Selfsigned oder CT_SMPKI_Signed (entspricht dann dem GW_WAN_TLS_CRT).
- Das SMGW **MUSS** in der Lage sein, zwei SMGW-HAN-Zertifikate mit zugehörigen Schlüsselpaaren für die TLS-Authentisierung zu verwenden. [REQ.HAN.SicherungKommunikation.60]
- Das SMGW **MUSS**+ die Verwendung des TLS-Zertifikates des SMGW aus der SM-PKI zur Authentisierung als GW_HAN_TLS_CRT (CT_SMPKI_Signed) verwenden können. (▸ICS.HAN.SicherungKommunikation.10) [REQ.HAN.SicherungKommunikation.22]
- Das SMGW **MUSS** als TLS-Server und TLS-Client im HAN das aktuelle $GW_HAN_TLS_CRT_n$ zur Authentisierung verwenden (▸tlsCert), sofern der Kommunikationspartner nicht gemäß [DS] Kapitel TLS (TLS-Handshake Certificate Authorities) signalisiert, dass das zuvor verwendete $GW_HAN_TLS_CRT_{n-1}$ zur Authentifizierung des SMGW benötigt wird. [REQ.HAN.SicherungKommunikation.21]
- Das SMGW **MUSS** im TLS-Handshake Zertifikate des Kommunikationspartners der Rollen CON, CLS und SRV gemäß [DS] Kapitel HAN-Zertifikatsprofile vom Typ CT_Selfsigned validieren können. [REQ.HAN.SicherungKommunikation.40]
- Das SMGW **SOLL** im TLS-Handshake Zertifikate des Kommunikationspartners gemäß [DS] Kapitel HAN-Zertifikatsprofil vom Typ CT_CA_Signed validieren können, sofern ein HAN-Kommunikationsprofil mit ▸role gleich "SRV" konfiguriert ist. (▸ICS.ZertifikateHAN.Allgemein.20) [REQ.HAN.SicherungKommunikation.41]
- Das SMGW **MUSS** den Aufbau der TLS-Verbindung beenden, sofern das vom Kommunikationspartner präsentierte Zertifikat nicht den kryptographischen Anforderungen für HAN-Zertifikate aus [TR-03109-3] entspricht. [REQ.HAN.SicherungKommunikation.50]

- Das SMGW **MUSS** bei Erreichen der maximalen Sitzungsdauer gemäß [TR-03109-3] oder ▸maxSessionDuration (der größere Wert zählt), einen neuen Sitzungsschlüssel vereinbaren oder die TLS-Verbindung trennen. [REQ.HAN.Kommunikationsprofile.20]
- Das SMGW **MUSS** die ▸role und - sofern ▸role gleich "CON" die ▸userId - des für die erfolgreiche Authentifizierung verwendeten HAN-Kommunikationsprofils für die Zugriffsberechtigung gemäß ▸Anhang C auf die Ressourcen des SMGW verwenden. [REQ.HAN.Kommunikationsprofile.60]

Hinweis: Das aktuelle GW_WAN_TLS_CRT bzw. GW_HAN_TLS_CRT ist über ▸FA.ReadCertificate auslesbar.

Schließen von TLS-Verbindungen



REQ.HAN.Transport.80

Das SMGW **MUSS** die TLS-Verbindung gemäß Parametern des zugeordneten HAN-Kommunikationsprofils beenden, falls

- ▸keepOpen "true" ist, ▸idleTimeout > 0 und mehr als ▸idleTimeout Sekunden ohne TLS-Applikationsdatentransfer vergangen sind
- (Nicht für HKS.TLSPROXY.*) ▸keepOpen "false" ist und eine Applikations-Response vollständig vom Kommunikationspartner empfangen wurde bzw. an den Kommunikationspartner übermittelt wurde
- Die maximale Lebensdauer der TLS-Sitzung ▸maxSessionDuration erreicht wurde und für TLS1.3 die erfolgreiche Vereinbarung neuer Sitzungsschlüssel innerhalb der bestehenden TLS-Verbindung nicht erfolgt ist.
- Eine Anforderung zum Beenden der TLS-Verbindung wird vom Kommunikationspartner empfangen.
- Das mit der TLS-Verbindung verknüpfte HAN- oder Proxy-Kommunikationsprofil gelöscht wird.
- (HKS.TLSPROXY.*) ▸outboundConnection.keepOpen "true" ist, ▸outboundConnection.idleTimeout > 0 und mehr als ▸outboundConnection.idleTimeout Sekunden ohne TLS-Applikationsdatentransfer vergangen sind.
- (HKS.TLSPROXY.* für TLS1.2) Das Proxy-Kommunikationsprofil die maximale Lebensdauer der TLS-Sitzung ▸outboundConnection.maxSessionDuration erreicht wurde
- (HKS.TLSPROXY.* für TLS1.3) Die erfolgreiche Vereinbarung neuer Sitzungsschlüssel innerhalb der bestehenden TLS-Verbindung nicht innerhalb von ▸outboundConnection.maxSessionDuration erfolgt ist.

Für HKS.TLSPROXY.*: Das WAN-Kommunikationsprofil wird über ▸wanPeerRef aus dem Proxy-Kommunikationsprofil referenziert, dessen HAN-Kommunikationsprofil über ▸hanPeerRef referenziert wird.

(Nicht für HKS.TLSPROXY.CLI) Das SMGW **MUSS** nach dem Schließen der TCP/TLS-Verbindung innerhalb von höchstens 5 Sekunden erneut eine TCP/TLS-Verbindung auf dem gleichen Port annehmen können. [REQ.HAN.Transport.70]

ICS



ICS.HAN.SicherungKommunikation.10

Der GWH **MUSS** im ICS deklarieren, ob das SMGW das GW_WAN_TLS_CRT zur Authentisierung im HAN verwenden kann.



ICS.ZertifikateHAN.Allgemein.20

Der GWH **MUSS** im ICS deklarieren, ob das SMGW die Anforderungen an die CT_CA_Signed (Typ B) HAN-Zertifikatsprofile für SRV und SMGW für die vom SMGW erzeugten und verarbeiteten HAN-Zertifikate umsetzt.



ICS.HAN.Kommunikationsszenarien.10

Der GWH **MUSS** im ICS den TLS-Handshake Timeout (in Sekunden) für einen HAN-TLS-Verbindungsaufbau deklarieren.

4.4.5 HAN-Netzwerk-Schnittstellen

- Das SMGW **MUSS** eine für den Anschlussnutzer und Servicetechniker in der Einbausituation zugängliche, physische HAN-Schnittstelle besitzen. [REQ.HAN.PhysSchnittstelle.10] Bei der Zugänglichkeit ist zu berücksichtigen, dass der Anschlussnutzer im Regelfall keine Elektrofachkraft ist.
- Diese Schnittstelle **MUSS** als Ethernet-Schnittstelle mit einer Geschwindigkeit von mindestens 10 MBit/s, interoperabel mit 10Base-TX und 100Base-TX ausgelegt sein. [REQ.HAN.PhysSchnittstelle.20] 10Base-TX ist in [IEEE 802.3i] Clause 14 beschrieben. 100Base-TX ist in [IEEE 802.3u] Clause 25 beschrieben.
- Das SMGW **MUSS** IPv4 an der HAN-Schnittstelle unterstützen. [REQ.HAN.PhysSchnittstelle.30]
- Das SMGW **KANN** IPv6 an der HAN-Schnittstelle unterstützen. [REQ.HAN.PhysSchnittstelle.40]
- Das SMGW **MUSS** IP-Pakete mit IP Quell- oder Ziel-Adressen die nicht in ▸Tabelle 4.14 aufgeführt sind ignorieren. [REQ.HAN.PhysSchnittstelle.55] Damit soll ein direkter Datenfluss vom WAN ins HAN über das SMGW vermieden werden.
- Sofern das SMGW die IPv4 HAN-Schnittstellenadresse nicht durch statische Konfiguration oder DHCP erhalten hat, **MUSS** das SMGW die link-lokale, eindeutige IPv4 HAN-Schnittstellenadresse spätestens 30 Sekunden nach Erkennen eines Ethernet-Links mittels "Dynamic Configuration of IPv4 Link-Local Addresses“ nach [RFC3927] und ARP-Probes nach [RFC826] bestimmen. [REQ.HAN.Network.30] Die Konfiguration der IP-Adresse der HAN-Schnittstelle ist in ▸Tabelle 3.82 und ▸FA.UpdateHanIfProfile beschrieben. DHCP-Adressbezug ist nicht im HAN-CLS zu verwenden.
- (IPv6 gemäß ▸ICS.HAN.PhysSchnittstelle.10) Das SMGW **MUSS** die IPv6 IP-Adressvereinbarung nach mit Stateless Address Auto-Configuration (SLAAC) nach [RFC4862] implementieren. [REQ.HAN.Network.40]
- (Keine HAN-Separation gemäß ▸ICS.HAN.PhysSchnittstelle.40) Das SMGW **MUSS** die IP-Adressparameter gemäß ▸hostIpv4Addr für das HAN-Netzwerk berücksichtigen. [REQ.HAN.PhysSchnittstelle.61]
- (HAN-Separation gemäß ▸ICS.HAN.PhysSchnittstelle.40) Das SMGW **MUSS** die IP-Adressparameter gemäß ▸hostIpv4Addr für das HAN-CON- und HAN-CLS-Netzwerk berücksichtigen. [REQ.HAN.PhysSchnittstelle.71]
- (HAN-Separation gemäß ▸ICS.HAN.PhysSchnittstelle.40) Das SMGW **DARF KEINE** Ethernet-Frames und IP-Pakete von einer physischen HAN-Schnittstelle zu einer weiteren lokalen physischen Schnittstelle weiterleiten. Sowohl ein Weiterleiten auf Layer 3 (IP-Routing) als auch ein Weiterleiten auf Layer 2 (MAC-Switching) sind nicht zulässig. Dies gilt insbesondere für IPv4-, IPv6-, ARP- und VLAN-Frames. [REQ.HAN.PhysSchnittstelle.80] Eine Kommunikation der Teilnehmer eines Netzwerkes untereinander ist zulässig.
- (HAN-Separation gemäß ▸ICS.HAN.PhysSchnittstelle.40) Das SMGW **MUSS** für HAN-CON den Bezug der IPv4-Adresse und Subnetzmaske mittels DHCP-Client unterstützen und auf die Private-Network-Bereiche gemäß [RFC1918] beschränken. [REQ.HAN.Network.70]

IP-Adressbereich	Beschreibung
192.168.0.0/16	IPv4 Private Network ([RFC1918])
172.16.0.0/12	IPv4 Private Network ([RFC1918]8)
10.0.0.0/8	IPv4 Private Network ([RFC1918])
169.254.0.0/16	IPv4 Link-Local Addresses ([RFC1918])
224.0.0.0/24	IPv4Local Network Multicast (RFC5771)
fc:00::/7	IPv6 Unique Local Addresses (RFC4193)
fe80::/10	IPv6 Link-Local Addresses ([RFC4291])

IP-Adressbereich	Beschreibung
ff02::/8	IPv6 Link Local Multicast Address ([RFC4291])

Tabelle 4.14 Übersicht der lokalen IP-Adressbereiche

ICS



ICS.HAN.PhysSchnittstelle.10

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



ICS.HAN.PhysSchnittstelle.40

Der GWH **MUSS** im ICS deklarieren, ob das SMGW eine von der HAN-CON-Netzwerkschnittstelle getrennte HAN-CLS-Netzwerkschnittstelle mit separater MAC-Adresse und IP-Adressbereich unterstützt.

Implementierungshinweis

Aufgrund möglicher doppelter Adresszuordnungen und Adresskonflikte wird von der Bereitstellung eines DHCP-Dienstes durch das SMGW im HAN-CON abgeraten.

Wird ein DHCP-Client im SMGW implementiert, soll dieser nur für den Bezug der IP-Hostadresse (und Subnetzmaske) verwendet werden und Gateway-Adresse und DHCP-Optionen sollen ignoriert werden.

4.4.6 Kommunikationsszenario HKS.WS1: Webservices des SMGW mit Authentifizierung durch TLS-Client-Zertifikat

4.4.6.1 Beschreibung

Das HKS.WS1 fasst die Protokolle und Nachrichtenformate zusammen, über die das SMGW an seiner HAN-Schnittstelle Webservices anbietet, damit berechtigte Nutzer im HAN auf die für sie bereitgestellten Dienste zugreifen können. Der Nutzer wird über ein im SMGW konfiguriertes TLS-Client-Zertifikat authentifiziert und autorisiert. Im Anwendungsprotokoll werden nur Daten übermittelt, für die der jeweils authentifizierte Nutzer berechtigt ist.

Dieses KS besteht aus folgenden Protokollen:

- Verbindungsorientiertes Transportprotokoll TCP mit im SMGW ankommenden Verbindungen.
- TLS für das SMGW in der Rolle des Servers, um vertrauliche und authentische Transportverbindungen zwischen SMGW und einem Kommunikationspartner zu gewährleisten.
- HTTP nach den Anforderungen für RESTful Webservices für das SMGW in der Rolle des Servers.

Das SMGW verwendet im TLS-Handshake das Geräteindividuelle GW_HAN_TLS_CRT gemäß Detailspezifikation "HAN-Zertifikatsprofile". Das GW_HAN_TLS_CRT kann dem GW_WAN_TLS_CRT entsprechen.

Das SMGW bietet dem Nutzer seine Dienste über ein Webservice-API vorzugsweise auf Port 443 (https) an. Dem Webservice-Zugriff über HTTP liegt das REST-Konzept zugrunde, bei dem ein uniformer (kleiner) Satz von Zugriffs-Verben auf verschiedene Ressourcen angewandt werden kann. Die Ressourcen können jeweils von unterschiedlichem Inhaltstyp (Content-Type) sein. Darüber hinaus bietet das SMGW Dienste zum Aufruf von Funktionen über das Webservice-API an.

▸Abbildung 4.19 verdeutlicht den Ablauf des HKS.WS1.

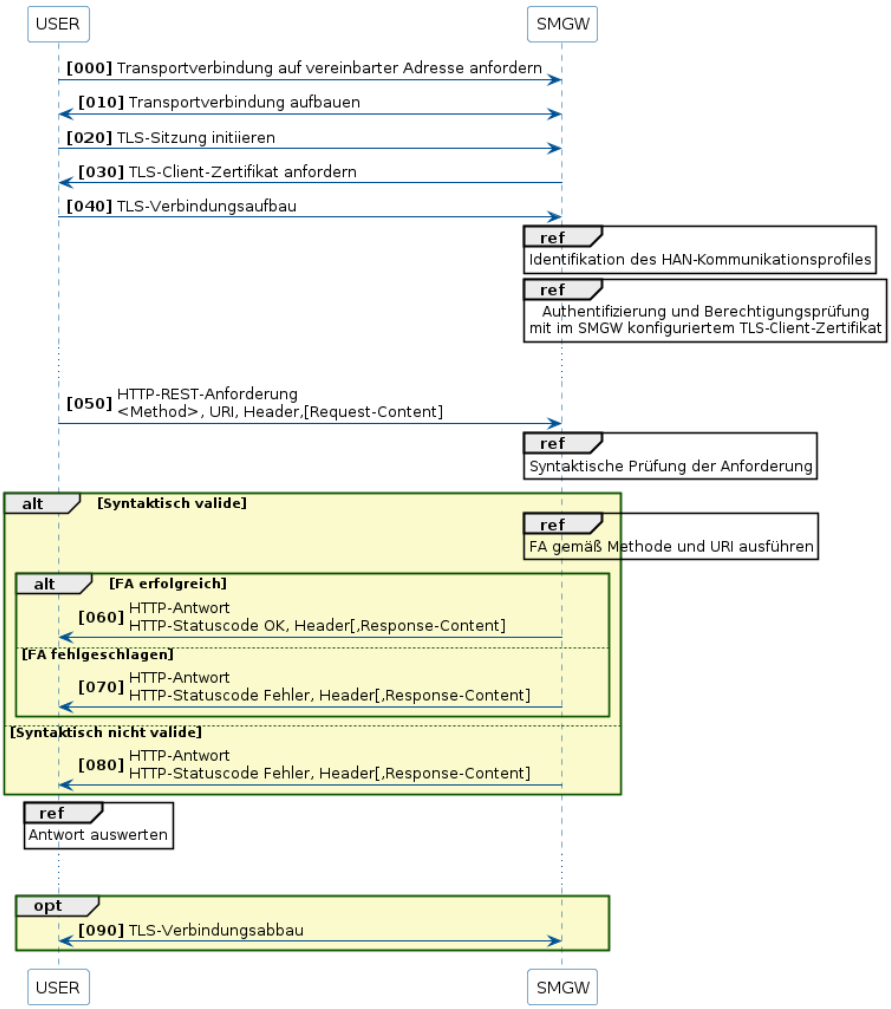


Abbildung 4.19. Authentifizierung des Nutzers im HAN mittels TLS-Client-Zertifikat

4.4.6.2 Vorbedingungen

- Das TLS-Client-Zertifikat zur Authentifizierung und Berechtigungsprüfung des Nutzers ist zuvor vom GWA im SMGW konfiguriert worden.
- Dem Kommunikationspartner des SMGW ist die Kommunikationsadresse (IP, Port) des SMGW bekannt, zu der die TLS-Verbindung für dieses HKS aufgebaut wird.

4.4.6.3 Anforderungen an die Kommunikationsprotokolle

Das Kommunikationsszenario HKS.WS1 verwendet die in ▸Tabelle 4.15 beschriebenen technische Anwendungsfälle der Kommunikationsprotokolle mit den über ein HAN-Kommunikationsprofil vom Typ "WS1" definierten Parametern.

Aufgabe	Detailspezifikation	Anforderungen
Annehmen einer Transport-Verbindung (ankommende Verbindung)	-	Das SMGW **MUSS** einen TCP-Verbindungsaufbau gemäß [RFC9293] in der Rolle des Acceptors (Passive Open) auf dem in ▸httpsPort angegebenen TCP-Port an der HAN-Schnittstelle durchführen können. [REQ.H-KS.WS1.10]

Aufgabe	Detailspezifikation	Anforderungen
Öffnen einer TLS-Session als Server	[DS] Kapitel "TLS" TA.TLS.OpenHanSessionAsServer, TA.TLS.Handshake	Anforderungen an die TLS-Authentifizierung zwischen SMGW und HAN-Kommunikationspartner sind in ▸Abschnitt 4.4.4 beschrieben. • Das SMGW **MUSS** TLS gemäß [DS] Kapitel TLS in der Rolle des Servers verwenden. [REQ.HAN.HKS1.11] • Das SMGW **MUSS** den TLS-Verbindungsaufbau mit TLS-Alert beenden, sofern kein HAN-Kommunikationsprofil konfiguriert ist, mit dessen ▸peerCert das im TLS-Handshake empfangene TLS-Client-Zertifikat validiert werden kann. ▸ [FNN.5002.1] [REQ.HAN.HKS1.20] • Sofern das vom Kommunikationspartner präsentierte SRV_HAN_TLS_CRT-Zertifikat vom Typ CA_CA_Signed (Typ B) ist **MUSS** das SMGW den TLS-Verbindungsaufbau mit einem TLS-Alert beenden, wenn das ▸peerCert Aussteller-CA-Zertifikat zeitlich nicht gültig ist oder das SRV_HAN_TLS_CRT nicht damit validiert werden kann. [REQ.HAN.HKS1.50] • Das SMGW **MUSS** die ▸userId des für die Authentifizierung des der TLS-Verbindung zugeordneten HAN-Kommunikationsprofiles für die Autorisierung des Zugriffs auf die der "userId" zugeordneten Ressourcen verwenden. ▸ [FNN.5002.0] [REQ.HAN.HKS1.60]
Verarbeiten und Erzeugen einer HTTP-Anfrage	[DS] Kapitel "RESTful Webservice" Anforderungen an HTTP-Server	Das SMGW **MUSS** den Zugriff auf Ressourcen des SMGW mit dem Protokoll gemäß [DS] Kapitel "RESTful Webservice" als HTTP-Server unterstützen. [REQ.HAN.Webservice.10] Das SMGW **MUSS** Webservice-Request und -Response für die ▸role gleich "CON" mit ▸ks gleich "WS1" gemäß Anlage Webservice-API - SMGW-API 2.0 für den Anschlussnutzer implementieren. [REQ.HAN.Webservice.70] Das SMGW **MUSS** Webservice-Request und -Response für die ▸role gleich "SRV" mit ▸ks gleich "WS1" gemäß Anlage Webservice-API - SMGW-API 2.0 für den Servicetechniker implementieren. [REQ.HAN.Webservice.71] Das SMGW **MUSS** Webservice-Request und -Response für die ▸role gleich "CLS" mit ▸ks gleich "WS1" gemäß Anlage Webservice-API - SMGW-API 2.0 für CLS implementieren. [REQ.HAN.Webservice.72]
		Das SMGW **SOLL** innerhalb von 10s beginnen eine Anfrage zu beantworten. [REQ.HKS.WS1.20] Das SMGW **MUSS** den Versuch eines unberechtigten Zugriffes auf eine (Webservice)-Ressource unmittelbar mit einer Fehlermeldung beenden. [REQ.HAN.Webservice.20] Das SMGW **MUSS** im Content-Type-Header der Webservice-Response mitteilen, welche Struktur die Inhaltsdaten besitzen. [REQ.HAN.Webservice.30] Das SMGW **MUSS** gemäß ▸keepOpen nach Versand der HTTP-Response die TLS-Verbindung geöffnet lassen (HTTP Connection: keep-alive). [REQ.HKS.WS1.21]

Tabelle 4.15 Anforderungen an die Protokolllayer des HKS.WS1

ICS



ICS.HAN.SicherungKommunikationConSrv.40

Der GWH **MUSS** im ICS deklarieren, ob das SMGW die Authentifizierung des Servicetechnikers mit kurzlebigen Zertifikaten ausgestellt durch eine CA gemäß [DS] Kapitel HAN-Zertifikatsprofile unterstützt.



ICS.HAN.SicherungKommunikationConSrv.70

Der GWH **MUSS** im ICS deklarieren, nach welcher Zeit (in Sekunden) das SMGW spätestens in HKS.WS1 beginnt einen HTTP-Request mit einer HTTP-Response zu beantworten.

ICS.HAN.SicherungKommunikationConSrv.80

Der GWH **MUSS** im ICS deklarieren, wie das Verhalten des SMGW bei Erreichen der maximalen TLS-Sitzungsdauer ist.

4.4.7 Kommunikationsszenario HKS.WS2: Webservices des SMGW mit Authentifizierung durch Nutzerkennung und Passwort

4.4.7.1 Beschreibung

Das HKS.WS2 fasst die Protokolle und Nachrichtenformate zusammen, über die das SMGW an seiner HAN-Schnittstelle Webservices anbietet, damit Anschlussnutzer im HAN auf die für sie bereitgestellten Dienste zugreifen können. Der Anschlussnutzer wird über eine im SMGW konfigurierte Benutzerkennung identifiziert und einen Hash aus Benutzerkennung und Passwort authentifiziert. Im Anwendungsprotokoll werden nur Daten übermittelt, für die der jeweils authentifizierte Anschlussnutzer berechtigt ist.

Dieses KS besteht aus folgenden Protokollen:

- Verbindungsorientiertes Transportprotokoll TCP mit im SMGW ankommenden Verbindungen.
- TLS für das SMGW in der Rolle des Servers, um vertrauliche und authentische Transportverbindungen zwischen SMGW und einem Kommunikationspartner zu gewährleisten.
- HTTP nach den Anforderungen für RESTful Webservices für das SMGW in der Rolle des Servers. Verwendet wird die Digest-Authentifizierung zur Nutzerauthentifizierung.

Das SMGW verwendet im TLS-Handshake das geräteindividuelle GW_HAN_TLS_CRT gemäß Detailspezifikation "HAN-Zertifikatsprofile". Das GW_HAN_TLS_CRT kann dem aus der SM-PKI stammenden GW_WAN_TLS_CRT entsprechen.

Bis auf die Methode zur Nutzerauthentifizierung entspricht das HKS.WS2 dem ▸HKS.WS1.

▸Abbildung 4.20 verdeutlicht den Ablauf des HKS.WS2.

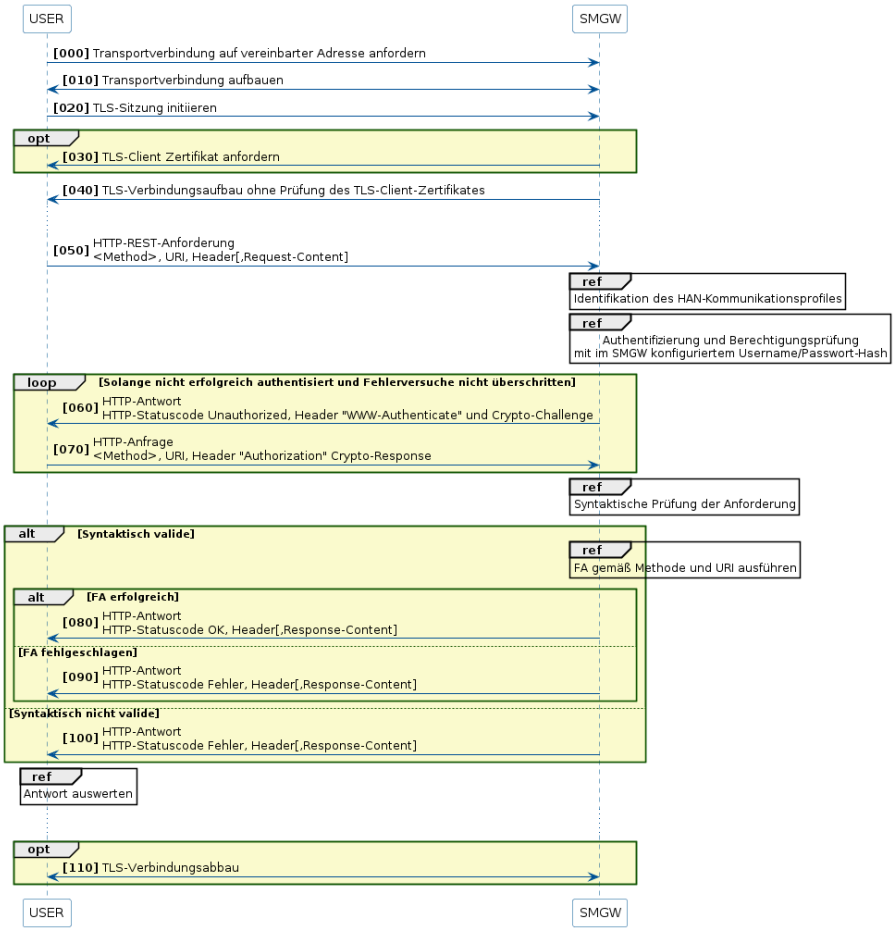


Abbildung 4.20. Authentifizierung des Anschlussnutzers im HAN mittels Nutzerkennung und Passwort

4.4.7.2 Vorbedingungen

- Die Nutzerkennung und der Hash über Nutzerkennung und Passwort zur Berechtigungsprüfung des Anschlussnutzers ist zuvor vom GWA im SMGW konfiguriert worden.
- Dem Kommunikationspartner im HAN ist die Kommunikationsadresse (IP, Port) des SMGW bekannt, zu der die TLS-Verbindung für dieses HKS aufgebaut wird.
- Die initial konfigurierte Nutzerkennung und das aktuelle Passwort zur Berechtigungsprüfung des Anschlussnutzers ist dem Kommunikationspartner bekannt.

4.4.7.3 Anforderungen an die Kommunikationsprotokolle

Das Kommunikationsszenario HKS.WS2 verwendet die in ▸Tabelle 4.16 beschriebenen technische Anwendungsfälle der Kommunikationsprotokolle mit den über ein HAN-Kommunikationsprofil vom Typ "WS2" definierten Parametern.

Aufgabe	Detailspezifikation	Anforderungen
Annehmen einer Transport-Verbindung (ankommende Verbindung)	-	Das SMGW **MUSS** einen TCP-Verbindungsaufbau gemäß [RFC9293] in der Rolle des Acceptors (Passive Open) auf dem in ▸httpsPort angegebenen TCP-Port an der HAN-Schnittstelle durchführen können. [REQ.HKS.WS2.10]
Öffnen einer TLS-Session als Server	[DS] Kapitel "TLS" TA.TLS.OpenHanSessionAsServer, TA.TLS.Handshake	Anforderungen an die TLS-Authentifizierung zwischen SMGW und HAN-Kommunikationspartner sind in ▸Abschnitt 4.4.4 beschrieben. Das SMGW **MUSS** TLS gemäß [DS] Kapitel TLS in der Rolle des Servers verwenden. [REQ.HAN.HKS2.21]

Aufgabe	Detailspezifikation	Anforderungen
Verarbeiten einer HTTP-Anfrage	[DS] Kapitel "RESTful Webservice" Anforderungen an HTTP-Server und Kapitel "HTTP-Authentifizierungs-Protokoll"	Das SMGW **MUSS** eine Authentifizierungsanforderung (Challenge) gemäß [DS] Kapitel "HTTP-Authentifizierungsprotokoll" gemäß der in den HAN-Kommunikationsprofilen genannten Authentifizierungsschemata ▸userCredentials.authScheme erzeugen (Bedingung: ▸authFailWait Wartezeit nicht aktiv.) [REQ.HAN.HKS2.23] Das SMGW **MUSS** die Anzahl der aufeinanderfolgenden, erfolglosen Authentifizierungsversuche in ▸HKS.WS2 auf ▸authAttempts beschränken, indem für einen Zeitraum von ▸authFailWait Sekunden keine weiteren Authentifizierungsversuche akzeptiert werden. [REQ.HAN.SicherungKommunikationConSrv.70] Das SMGW **MUSS** die ▸userId des für die Authentifizierung verwendeten HAN-Kommunikationsprofiles für Autorisierung des Zugriffs auf die der "userId" zugeordneten Ressourcen verwenden. ▸ [FNN.5001.0] [REQ.HAN.HKS2.60] Das SMGW **MUSS** den Zugriff auf Ressourcen des SMGW mit dem Protokoll gemäß [DS] Kapitel "RESTful Webservice" als HTTP-Server unterstützen. [REQ.HAN.Webservice.11] Das SMGW **MUSS** Webservice-Request und -Response für die ▸role gleich "CON" mit ▸ks gleich "WS2" gemäß Anlage Webservice-API - SMGW-API 2.0 für den Endkunden implementieren. [REQ.HAN.Webservice.73]
Erzeugen einer HTTP-Antwort und json-Nachricht	[DS] Kapitel "RESTful Webservice" Anforderungen an HTTP-Server	Das SMGW **MUSS** den HTTP-Request mit einem Autorisierungsfehler ablehnen und die TLS-Verbindung beenden, sofern die empfangenen Credentials mit keinen der in den HAN-Kommunikationsprofilen genannten Username/Passwort-Hash-Credentials ▸userCredentials übereinstimmen. ▸ [FNN.5001.1] [REQ.HAN.HKS2.30] Das SMGW **MUSS** gemäß ▸keepOpen nach Versand der HTTP-Response die TLS-Verbindung geöffnet lassen (HTTP Connection: keep-alive). [REQ.HKS.WS2.21]

Tabelle 4.16 Anforderungen an die Protokolllayer des HKS.WS2

4.4.8 Kommunikationsszenario HKS.TLSPROXY.SOCKS: TLS-SOCKS-Proxy-Verbindung initiiert durch CLS

4.4.8.1 Beschreibung

Dieses HKS fasst die Protokolle und Nachrichtenformate zusammen, über die das SMGW an seiner HAN-Schnittstelle Dienste anbietet, damit ein CLS eine Proxy-Verbindung mit dem SOCKS-Protokoll über das SMGW zu einem aEMT aufbauen kann.

Beim Aufbau einer TLS-Verbindung vom CLS zum SMGW an die zuvor vereinbarte Kommunikationsadresse übermittelt das CLS dem SMGW über das SOCKS-Protokoll die Identifikation des aktiven EMT, zu dem eine TLS-Proxy-Verbindung hergestellt werden soll (Bisher HKS3).

Dieses KS besteht aus folgenden Protokollen:

- Verbindungsorientiertes TCP-Transportprotokoll in der Rolle des Verbindungs-Empfängers, um eine zuverlässige und interoperable Transportverbindung zwischen einem Nutzer im HAN und dem SMGW herzustellen.
- TLS für das SMGW in der Rolle des Servers, um vertrauliche und authentische Transportverbindungen zwischen einem Nutzer im HAN und dem SMGW zu gewährleisten.
- SOCKS-Protokoll zur Signalisierung von Informationen zur Auswahl des im SMGW konfigurierten Proxy-Kommunikationsprofils.

Das SMGW bietet dem CLS seinen Vermittlungsdienst über den SOCKS-Port an.

▸Abbildung 4.21 und ▸Abbildung 4.22 verdeutlicht den Ablauf der im HKS.TLSPROXY.SOCKS verwendeten Kommunikationsdienste SOCKS-Verbindungsaufbau, TLS-Verbindungsaufbau, Transparenter Datenaustausch zwischen CLS, SMGW und aktivem EMT und den TLS-Verbindungsabbau.

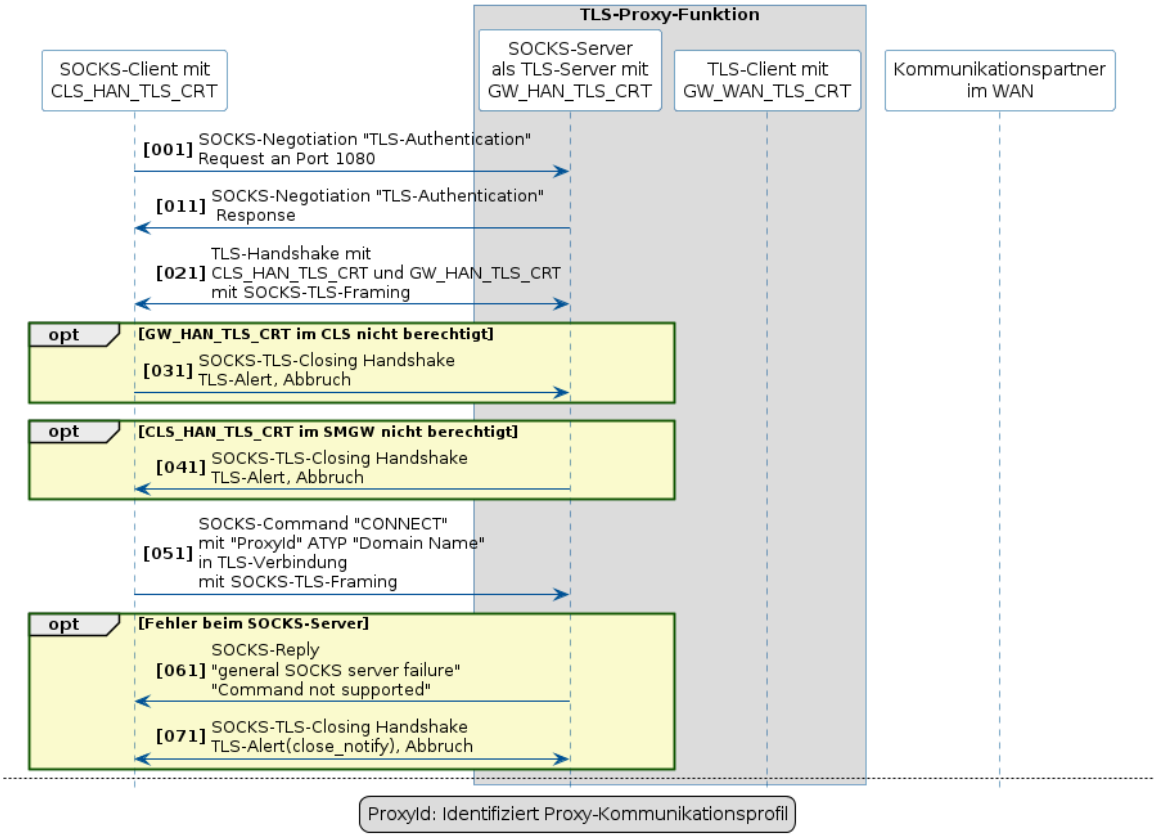


Abbildung 4.21. Übersicht über den Ablauf des HKS.TLSPROXY.SOCKS (1/2)

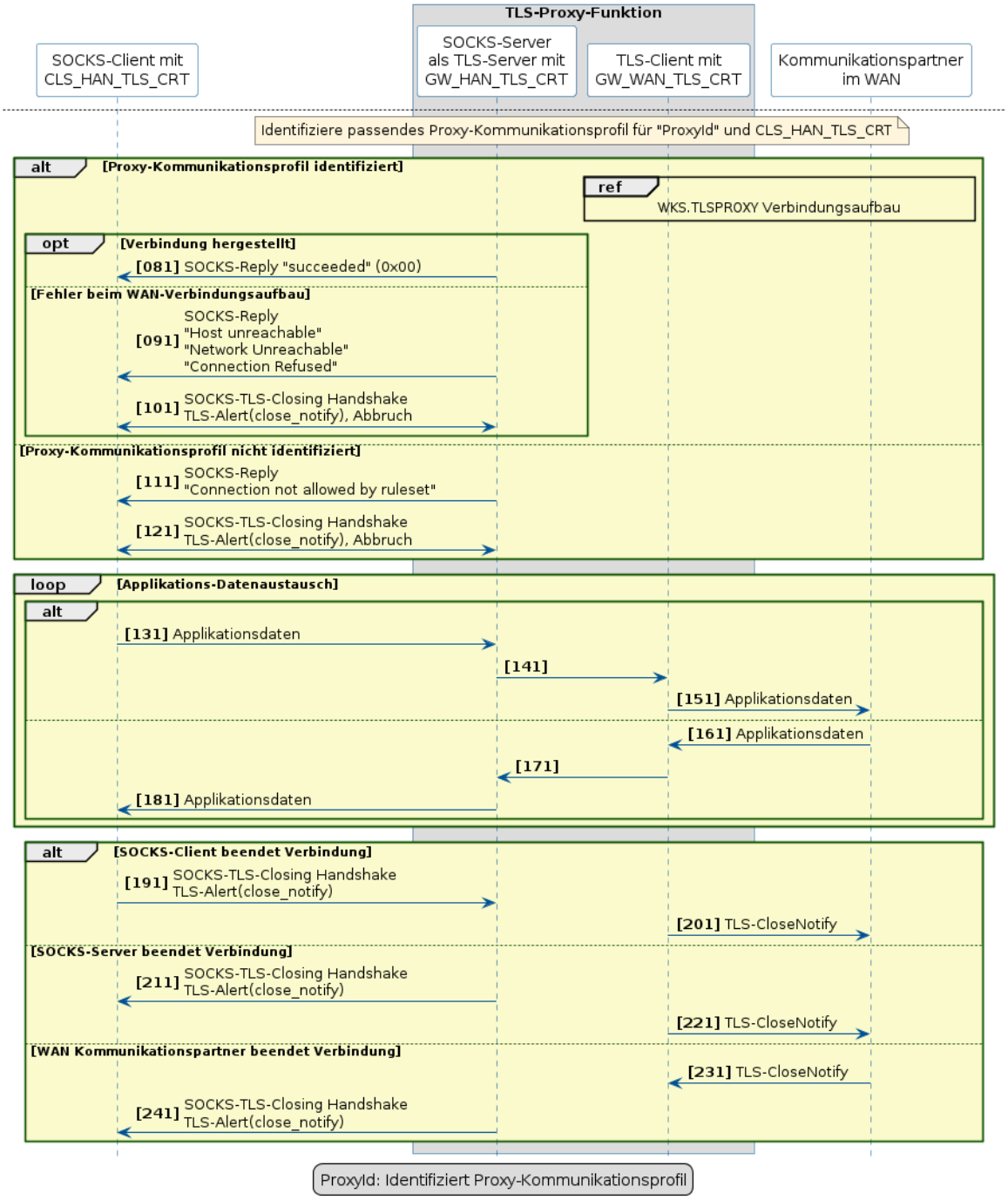


Abbildung 4.22. Übersicht über den Ablauf des HKS.TLSPROXY.SOCKS (2/2)

4.4.8.2 Vorbedingungen

- Das HAN-Kommunikationsprofil mit dem TLS-Client-Zertifikat zur Authentifizierung und Berechtigungsprüfung des CLS ist zuvor vom GWA im SMGW konfiguriert worden.
- Das WAN-Kommunikationsprofil für den Verbindungsaufbau zum aktiven EMT ist zuvor vom GWA im SMGW konfiguriert worden.
- Das Proxy-Kommunikationsprofil für den Verbindungsaufbau vom CLS und zum aktiven EMT ist zuvor vom GWA im SMGW konfiguriert worden.
- Dem CLS ist die Kommunikationsadresse (IP) des SMGW bekannt, zu der die TLS-Verbindung für dieses HKS aufgebaut wird.

4.4.8.3 Anforderungen an die Kommunikationsprotokolle

Das Kommunikationsszenario HKS.TLSPROXY.SOCKS verwendet die in ▸Tabelle 4.17 beschriebenen technische Anwendungsfälle der Kommunikationsprotokolle mit den über ein Proxy-Kommunikationsprofil vom Typ "TLSPROXY.SOCKS" definierten Parametern.

Das in der folgenden Tabelle referenzierte HAN-Kommunikationsprofil ist immer das über ▸hanPeerRef referenzierte HAN-Kommunikationsprofil vom Typ "TLSPROXY.SOCKS".

Das in der folgenden Tabelle referenzierte WAN-Kommunikationsprofil ist das über ▸wanPeerRef referenzierte WAN-Kommunikationsprofil vom Typ "TLSPROXY".

Aufgabe	Detailspezifikation	Anforderungen
Annehmen einer Transport-Verbindung (ankommende Verbindung)	-	Das SMGW **MUSS** einen TCP-Verbindungsaufbau gemäß [RFC9293] in der Rolle des Acceptors (Passive Open) auf dem in ▸socksPort angegebenen TCP-Port an der HAN-Schnittstelle durchführen können. Default Port ist 1080. [REQ.HKS.TLSPROXY.SOCKS.10]
Öffnen einer SOCKS-TLS-Session als Server	[DS] Kapitel "SOCKS-TLS-Protokoll" TA.SOCKSTLS.NegotiateAuth, TA.SOCKSTLS.Connect	Anforderungen an die TLS-Authentifizierung zwischen SMGW und HAN-Kommunikationspartner sind in ▸Abschnitt 4.4.4 beschrieben. Das SMGW **MUSS** das SOCKS/TLS-Protokoll in der Rolle des Servers gemäß [DS] Kapitel "SOCKS-TLS-Protokoll" implementieren. [REQ.HKS.TLSPROXY.SOCKS.20] Das SMGW **MUSS** den SOCKS-TLS-Verbindungsaufbau mit Fehler-Response beenden, sofern kein HAN-Kommunikationsprofil vom Typ ▸ks gleich "TLSPROXY.SOCKS" konfiguriert ist, dessen ▸peerCert mit dem im TLS-Handshake empfangenen TLS-Client-Zertifikat und dessen ▸wanPeerRef mit dem im SOCKS-CONNECT empfangenen dnsName gleich ▸wanPeerRef oder der im SOCKS-CONNECT empfangenen IP-Adresse und Port-Nummer gemäß ▸outboundConnection.addresses übereinstimmt. ▸ [FNN.5003.2] [REQ.HKS.TLSPROXY.SOCKS.30] Siehe ▸FA.RequestProxyChByCls.

Tabelle 4.17 Anforderungen an die Protokolllayer des HKS.TLSPROXY.SOCKS

4.4.9 Kommunikationsszenario HKS.TLSPROXY.SRV: TLS-Proxy-Verbindung initiiert durch CLS

4.4.9.1 Beschreibung

Dieses HKS fasst die Protokolle und Nachrichtenformate zusammen, über die das SMGW an seiner HAN-Schnittstelle Dienste anbietet, damit ein CLS eine Proxy-Verbindung über das SMGW zu einem aEMT aufbauen kann.

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

Dieses KS besteht aus folgenden Protokollen:

- Verbindungsorientiertes TCP/IP-Transportprotokoll in der Rolle des Verbindungs-Empfängers, um eine zuverlässige und interoperable Transportverbindung zwischen einem Nutzer im HAN und dem SMGW herzustellen.
- TLS für das SMGW in der Rolle des Servers, um vertrauliche und authentische Transportverbindungen zwischen einem Nutzer im HAN und dem SMGW zu gewährleisten.
- Signalisierung von Informationen zur Auswahl des im SMGW konfigurierten Proxy-Kommunikationsprofils.

Das SMGW bietet dem CLS seinen Vermittlungsdienst über einen, dem CLS bekannten TCP-Port, der im Proxy-Kommunikationsprofil festgelegt ist, an.

Abbildung 4.23 verdeutlicht den Ablauf der im HKS.TLSPROXY.SRV verwendeten Kommunikationsdienste TLS-Verbindungsaufbau, Transparenter Datenaustausch zwischen CLS, SMGW und aktivem EMT und den TLS-Verbindungsabbau.

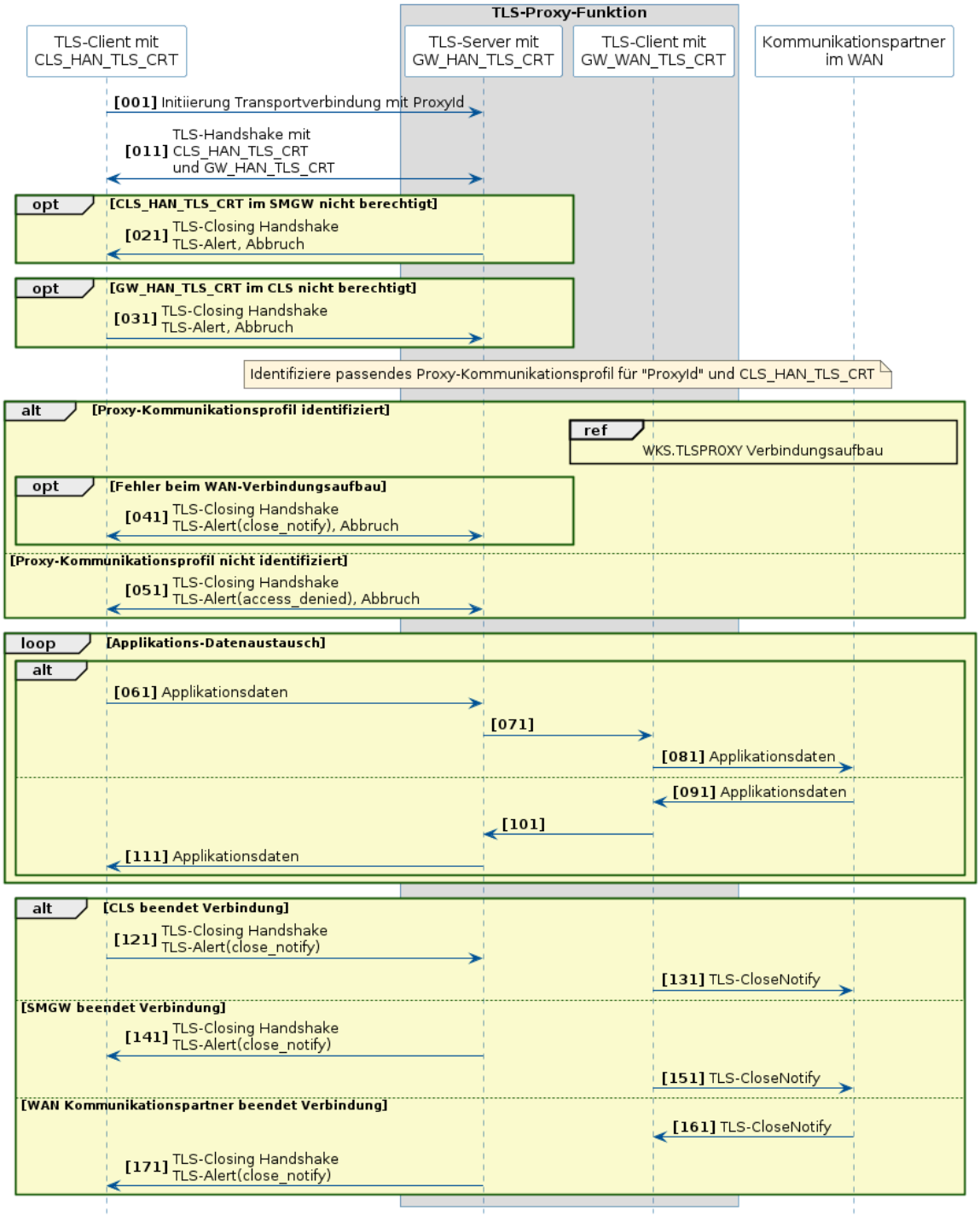


Abbildung 4.23. Übersicht über den Ablauf des HKS.TLSPROXY.SRV

4.4.9.2 Vorbedingungen

- Das HAN-Kommunikationsprofil mit dem TLS-Client-Zertifikat zur Authentifizierung und Berechtigungsprüfung des CLS ist zuvor vom GWA im SMGW konfiguriert worden.
- Das WAN-Kommunikationsprofil für den Verbindungsaufbau zum aktiven EMT ist zuvor vom GWA im SMGW konfiguriert worden.
- Das Proxy-Kommunikationsprofil für den Verbindungsaufbau vom CLS zum aktiven EMT ist zuvor vom GWA im SMGW konfiguriert worden.

- Dem CLS ist die Kommunikationsadresse (IP, Port) des SMGW bekannt, zu der die TLS-Verbindung für dieses HKS aufgebaut wird.

4.4.9.3 Anforderungen an die Kommunikationsprotokolle

Das Kommunikationsszenario HKS.TLSPROXY.SRV verwendet die in ▸Tabelle 4.18 beschriebenen technische Anwendungsfälle der Kommunikationsprotokolle mit den über ein Proxy-Kommunikationsprofil vom Typ "TLSPROXY.SRV" definierten Parametern.

Das in der folgenden Tabelle referenzierte HAN-Kommunikationsprofil ist immer das über ▸hanPeerRef referenzierte HAN-Kommunikationsprofil vom Typ "TLSPROXY.SRV".

Aufgabe	Detailspezifikation	Anforderungen
Annehmen einer Transport-Verbindung (ankommende Verbindung)		Das SMGW **MUSS** einen TCP-Verbindungsaufbau gemäß [RFC9293] in der Rolle des Acceptors (Passive Open) auf dem in ▸tlsProxyPort angegebenen TCP-Port an der HAN-Schnittstelle durchführen können. Default Port ist 31091. [REQ.HKS.TLSPROXY.SRV.10]
Öffnen einer TLS-Session als Server	[DS] Kapitel "TLS" TA.TLS.OpenHanSessionAsServer, TA.TLS.Handshake	Anforderungen an die TLS-Authentifizierung zwischen SMGW und HAN-Kommunikationspartner sind in ▸Abschnitt 4.4.4 beschrieben. Das SMGW **MUSS** TLS gemäß [DS] Kapitel TLS in der Rolle des Servers verwenden. [REQ.HKS.TLSPROXY.SRV.20] Das SMGW **MUSS** den TLS-Verbindungsaufbau mit TLS-Alert beenden, sofern kein HAN-Kommunikationsprofil vom Typ ▸ks gleich "TLSPROXY.SRV" konfiguriert ist, dessen ▸peerCert mit dem im TLS-Handshake empfangenen TLS-Client-Zertifikat und dessen ▸wanPeerRef mit der empfangenen TLS-SNI übereinstimmt. ▸ [FNN.5003.2] [REQ.HKS.TLSPROXY.SRV.30] Siehe ▸FA.RequestProxyChByCls

Tabelle 4.18 Anforderungen an die Protokolllayer des HKS.TLSPROXY.SRV

4.4.10 Kommunikationsszenario HKS.TLSPROXY.CLI: TLS-Proxy-Verbindung zum CLS initiiert durch SMGW

4.4.10.1 Beschreibung

Das HKS.TLSPROXY.CLI fasst die Protokolle und Nachrichtenformate zusammen, über die das SMGW an seiner HAN-Schnittstelle eine Proxy-Verbindung zu einem CLS aufbauen kann (Bisher HKS4 und HKS5).

Diese KS besteht aus folgenden Protokollen:

- Verbindungsorientiertes TCP/IP-Transportprotokoll in der Rolle des Initiators, um eine zuverlässige und interoperable Transportverbindung zwischen dem SMGW und einem Nutzer im HAN herzustellen.
- TLS für das SMGW in der Rolle des Clients, um vertrauliche und authentische Transportverbindungen zwischen SMGW und einem berechtigten Nutzer im HAN (CLS) zu gewährleisten.

Das SMGW baut eine Verbindung zu einem CLS auf, dessen lokale Adresse im Proxy-Kommunikationsprofil festgelegt ist.

▸Abbildung 4.24 verdeutlicht den Ablauf der im HKS.TLSPROXY.CLI verwendeten Kommunikationsdienste TLS-Verbindungsaufbau, Transparenter Datenaustausch zwischen CLS, SMGW, aEMT und den TLS-Verbindungsabbau.

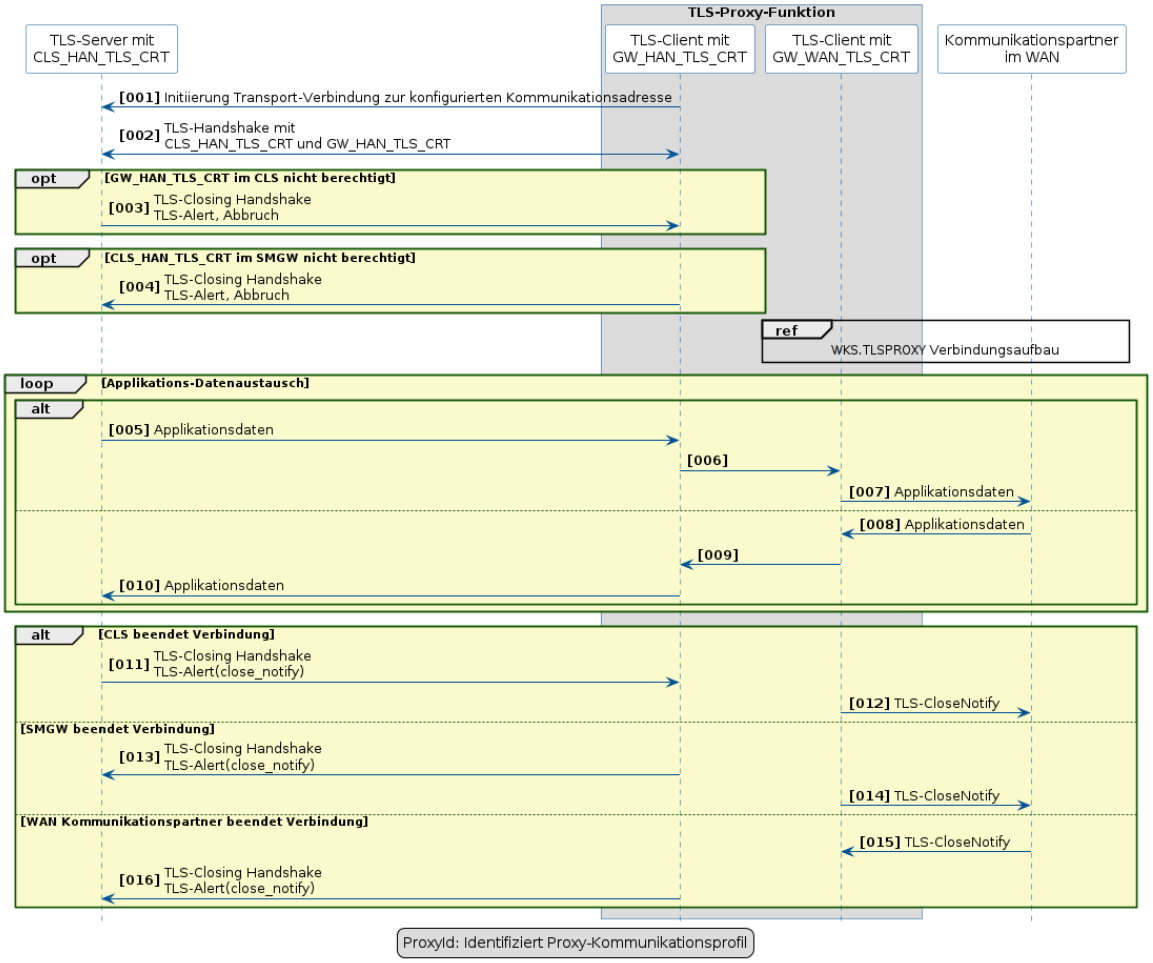


Abbildung 4.24. Übersicht über den Ablauf des HKS.TLSPROXY.CLI

4.4.10.2 Vorbedingungen

- Das HAN-Kommunikationsprofil mit dem TLS-Server-Zertifikat zur Authentifizierung und Berechtigungsprüfung des CLS ist zuvor vom GWA im SMGW konfiguriert worden.
- Das WAN-Kommunikationsprofil für den Verbindungsaufbau zum aktiven EMT ist zuvor vom GWA im SMGW konfiguriert worden.
- Das Proxy-Kommunikationsprofil für den Verbindungsaufbau zum CLS und zum aktiven EMT ist zuvor vom GWA im SMGW konfiguriert worden.
- Die Kommunikationsadresse (IP, Port) des CLS ist zuvor über ein Proxy-Kommunikationsprofil vom GWA im SMGW konfiguriert worden.

4.4.10.3 Anforderungen an die Kommunikationsprotokolle

Das Kommunikationsszenario HKS.TLSPROXY.CLI verwendet die in ▸Tabelle 4.19 beschriebenen technische Anwendungsfälle der Kommunikationsprotokolle mit den über ein Proxy-Kommunikationsprofil vom Typ "TLSPROXY.CLI" definierten Parametern.

Das in der folgenden Tabelle referenzierte HAN-Kommunikationsprofil ist immer das über ▸hanPeerRef referenzierte HAN-Kommunikationsprofil vom Typ "TLSPROXY.CLI" des auslösenden Proxy-Kommunikationsprofils.

Aufgabe	Detailspezifikation	Anforderungen
Aufbau einer Transport-Verbindung (abgehende Verbindung)		Das SMGW **MUSS** einen TCP-Verbindungsaufbau gemäß [RFC9293] in der Rolle des Initiators (Active Open) auf die in ▸outboundConnection.address angegebene IP-Adresse/TCP-Port an der HAN-Schnittstelle durchführen können. [REQ.HKS.TLSPROXY.CLI.10] Sofern der TCP-Verbindungsaufbau nicht innerhalb der über ▸outboundConnection.retryConfig definierten Zeit erfolgreich ist, **MUSS** das SMGW unmittelbar nach Ablauf dieser Zeit den nächsten Verbindungsaufbau initiieren, solange ▸outboundConnection.retryConfig.retryDelay noch nicht erreicht ist. [REQ.HKS.TLSPROXY.CLI.20] Das SMGW **MUSS** den Aufbau der Verbindung endgültig als fehlgeschlagen betrachten, sofern die Zahl der Wiederholversuche gemäß ▸outboundConnection.retryConfig erreicht wurde. ▸ [FNN.5003.1] [REQ.HKS.TLSPROXY.CLI.30]
Öffnen einer TLS-Session als Client	[DS] Kapitel "TLS" TA.TLS.OpenHanSessionAsClient, TA.TLS.Handshake	Anforderungen an die TLS-Authentifizierung zwischen SMGW und HAN-Kommunikationspartner sind in ▸Abschnitt 4.4.4 beschrieben. Das SMGW **MUSS** TLS gemäß [DS] Kapitel TLS in der Rolle des Clients verwenden. [REQ.HAN.HKS4.21] Das SMGW **MUSS** den TLS-Verbindungsaufbau mit TLS-Alert beenden, sofern das im TLS-Handshake empfangene TLS-Server-Zertifikat nicht mit ▸peerCert übereinstimmt. ▸ [FNN.5003.2] [REQ.HAN.HKS4.40] Das SMGW **MUSS** den ▸localServerName als ServerName im TLS-Handshake übermitteln, sofern das Datenfeld im Proxy-Kommunikationsprofil konfiguriert ist. [REQ.HAN.HKS4.41]

Tabelle 4.19 Anforderungen an die Protokolllayer des HKS.TLSPROXY.CLI

4.4.11 Kommunikationsszenario HKS.NTP-TLS.SRV: Zeitsynchronisation mit dem SMGW als NTP-TLS-Server

4.4.11.1 Beschreibung

Das HKS.NTP-TLS.SRV fasst die Protokolle und Nachrichtenformate für eine Zeitsynchronisation mittels NTP bzw. SNTP über TLS zusammen, über die das SMGW im HAN die Zeit für HAN-Teilnehmer bereitstellt. .

Dieses KS besteht aus folgenden Protokollen:

- Verbindungsorientiertes Transportprotokoll TCP mit ankommenden Verbindungen.
- TLS in der Rolle des Servers, um die Zeit authentisch an den Client zu übermitteln.
- NTP in der Rolle des Servers, um die Nachrichten zur Zeitsynchronisation auszutauschen.

▸Abbildung 4.25 verdeutlicht den Nachrichtenaustausch zwischen HAN-Teilnehmer und SMGW.

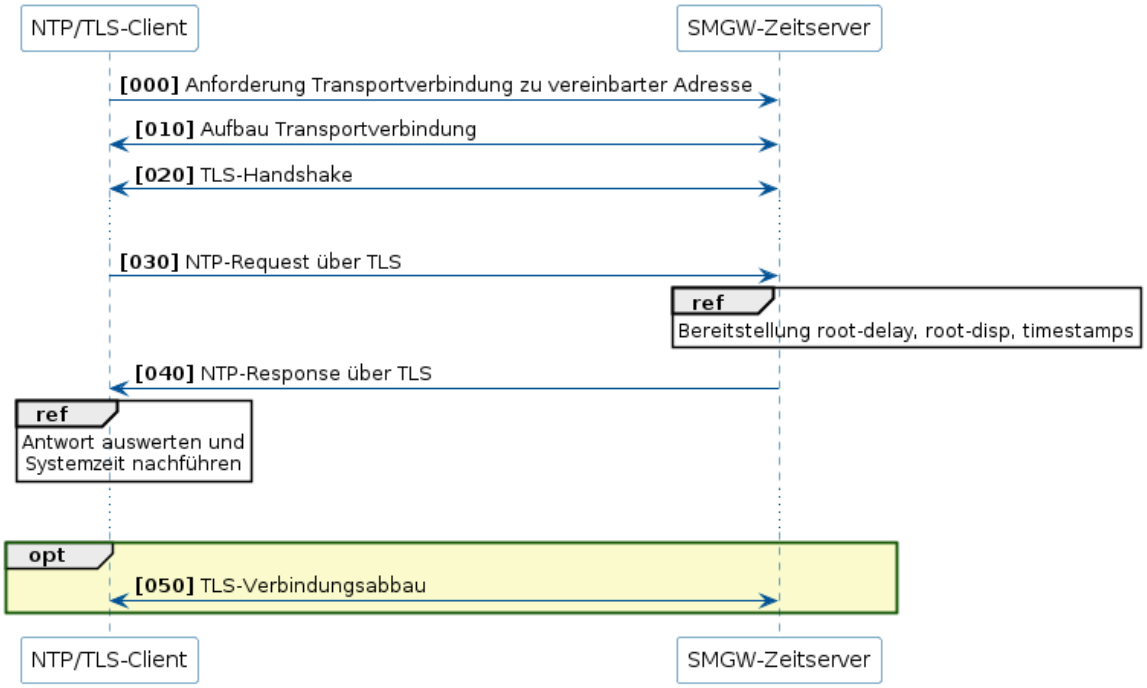


Abbildung 4.25. Übersicht über den Ablauf des HKS.NTP-TLS.SRV

Da eine 1:1 Zuordnung von NTP-Nachricht und TLS-Application-Record vorliegt und darüber hinaus die NTP-Nachrichten eine feste Länge haben, ist kein Adaptionslayer zwischen NTP und TLS notwendig.

4.4.11.2 Vorbedingungen

Das SMGW ist für den HAN-Teilnehmer kommunikativ erreichbar.

Die Kommunikationsadresse des SMGW und das akzeptierte TLS-Server-Zertifikat GW_HAN_TLS_CRT liegen im SMGW vor.

4.4.11.3 Anforderungen an die Kommunikationsprotokolle

Das Kommunikationsszenario HKS.NTP-TLS.SRV verwendet die in ▸Tabelle 4.20 beschriebenen technische Anwendungsfälle der Kommunikationsprotokolle mit den über ein HAN-Kommunikationsprofil vom Typ "NTP-TLS" definierten Parametern.

Aufgabe	Detailspezifikation	Anforderungen
Annehmen einer Transport-Verbindung (ankommende Verbindung)		Das SMGW **MUSS** einen TCP-Verbindungsaufbau gemäß [RFC9293] in der Rolle des Acceptors (Passive Open) auf dem in ▸ntpTlsPort vom Typ "NTP-TLS" angegebenen TCP-Port an der HAN-Schnittstelle durchführen können. Default-Port ist 4460. [REQ.HKS.NTP-TLS.SRV.10]
Öffnen einer TLS-Session als Server	[DS] Kapitel "TLS - Transport Layer Security Protokoll" TA.TLS.OpenHanSessionAsServer, TA.TLS.Handshake	Anforderungen an die TLS-Authentifizierung zwischen SMGW und HAN-Kommunikationspartner sind in ▸Abschnitt 4.4.4 beschrieben. Das SMGW **MUSS** TLS gemäß [DS] Kapitel "TLS" in der Rolle des Servers verwenden. [REQ.HKS.NTP-TLS.SRV.20]
Senden von TLS-Applikationsdaten		Sofern das SMGW im TLS-Handshake keine ALPN-Extension oder eine ALPN-Extension "ntp/4" empfangen hat, **MUSS** das SMGW die NTP-Nachrichten (Request/Response) ohne weitere vorangestellte oder nachfolgende Daten als TLS-Applikationsdaten übertragen und empfangen. [REQ.HKS.NTP-TLS.SRV.50]
Empfangen von TLS-Applikationsdaten		

Aufgabe	Detailspezifikation	Anforderungen
Verarbeiten einer NTP-Anfrage	[DS] Kapitel "NTP - Network Time Protokoll" TA.NTP.ProcessRequest, TA.NTP.BuildResponse	Das SMGW **MUSS** NTP gemäß [DS] in der Rolle des Servers verwenden. Eine Client-Authentifizierung ist nicht erforderlich. [REQ.H-KS.NTP-TLS.SRV.30]
Erzeugen einer NTP-Antwort		

Tabelle 4.20 Anforderungen an die Protokolllayer des HKS.NTP-TLS.SRV

4.4.12 HKS.DNSDISCOVERY

4.4.12.1 Beschreibung

Das HKS.DNSDISCOVERY unterstützt die interoperable und automatische Bestimmung und Bereitstellung einer Geräte- oder Dienstadresse und Geräteidentifikation mittels DNS im HAN des SMGW.

Das SMGW und CLS bieten HAN-Teilnehmern Dienste an der HAN-Schnittstelle an. Zur Nutzung der Dienste muss ein HAN-Teilnehmer Kenntnis der Link-, Netzwerk- und Transportadresse von Gerät und Dienst erhalten. Dies kann durch vorherige Konfiguration (statische Vereinbarung) oder automatisch durch (dynamische) Vereinbarung geschehen. Dieses HKS beschreibt die Protokolle für das automatische Auffinden von Komponenten im HAN.

Dieses KS besteht aus den folgenden Protokollen:

- Das SMGW verwendet UDP/IP mit Multicast zum Transport der mDNS und DNS-SD Nachrichten, sowie Link-, Netzwerk- und Transportprotokoll in der Rolle des Empfängers und Senders, um den verbindungslosen Transport im Netzwerk zum SMGW herzustellen.
- Das SMGW stellt an seiner HAN-Schnittstelle einen link-lokalen mDNS Responder und mDNS Querier gemäß [DS] Kapitel "mDNS" bereit, so dass HAN-Teilnehmer die Netzwerkadresse eines SMGW anhand einer bekannten *SMGW-ID* oder eines SMGW mit unbekannter SMGW-ID erhalten können. Es werden mDNS-Adressanfragen nach "<SMGW-ID>.local." und "smgw.local." mit der link-lokalen oder privaten Netzwerkadresse des SMGW beantwortet. Weiterhin stellt das SMGW mDNS Anfragen an CLS zur Identifikation der Geräte im HAN-CLS.
- Das SMGW implementiert einen DNS-Service Discovery Responder und Querier (DNS-SD) gemäß [RFC6763], um die Port-Nummern für die Diensttypen ("serviceTypes") des SMGW und eines CLS auf Anfrage zu erhalten und bereitzustellen.

▸Abbildung 4.26 verdeutlicht den Ablauf der Adressbestimmung über mDNS/DNS-SD.

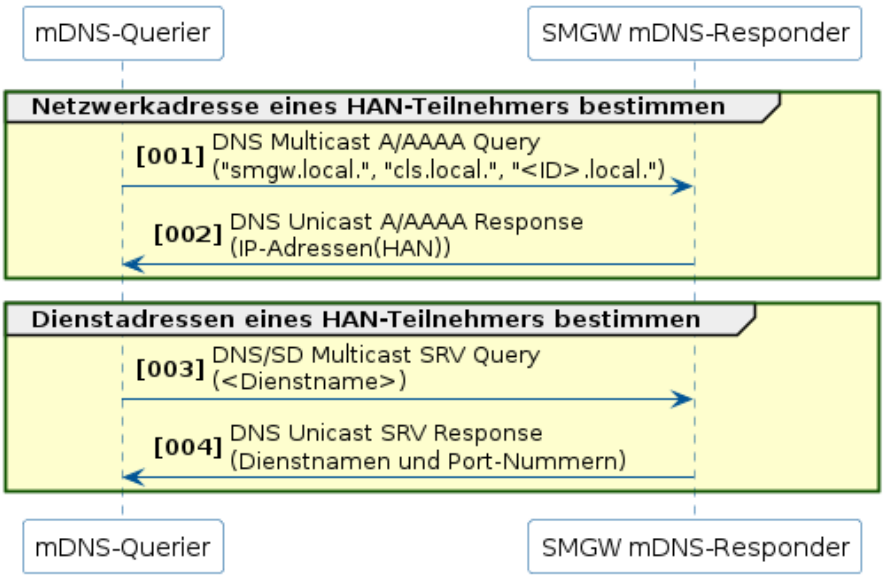


Abbildung 4.26. Übersicht über den Ablauf der automatischen Adressbestimmung im HAN

4.4.12.2 Anforderungen an die Kommunikationsprotokolle

Das Kommunikationsszenario HKS.DNSDISCOVERY verwendet die in ▸Tabelle 4.21 beschriebenen technische Anwendungsfälle der Kommunikationsprotokolle.

Aufgabe	Detailspezifikation	Anforderungen
Empfang und Senden einer UDP Nachricht		Das SMGW **MUSS** UDP Nachrichten gemäß [RFC768] auf IP-Adresse und Port gemäß [DS] Kapitel "mDNS - Device/Service Discovery Protokoll" entgegennehmen und senden können. [REQ.HKS.DNS.SRV.5]
mDNS Responder	[DS] Kapitel "mDNS - Device/Service Discovery Protokoll" TA.mDNS.Responder	Das SMGW **MUSS** mDNS Anfragen mit dem DNS Host-Namen "smgw.local." beantworten. [REQ.HKS.DNS.SRV.30] Das SMGW **MUSS** mDNS Anfragen mit dem DNS Host-Namen "<SMGW-ID>.local." beantworten, wobei die SMGW-ID gemäß [DIN43849] gebildet wird. [REQ.HKS.DNS.SRV.40] Das SMGW **MUSS** an der HAN-Schnittstelle gemäß [DS] Kapitel "mDNS - Device/Service Discovery Protokoll" die SMGW-HAN-Schnittstellenadresse für IPv4 bereitstellen. [REQ.HKS.DNS.SRV.10] (IPv6 gemäß ▸ICS.HAN.PhysSchnittstelle.10) Das SMGW **MUSS** an der HAN-Schnittstelle gemäß [DS] Kapitel "mDNS - Device/Service Discovery Protokoll" mindestens die Link-Lokale SMGW-HAN-Schnittstellenadresse für IPv6 bereitstellen. [REQ.HKS.DNS.SRV.20] Das SMGW **SOLL** die Anfrage nach Diensttypen tlsproxy, ntps, https mit den lokalen Portnummern der HAN- und Proxy-Kommunikationsprofile als mDNS-Responder mit DNS-SD gemäß [DS] Kapitel "mDNS - Device/Service Discovery Protokoll" beantworten. [REQ.HKS.DNS.SRV.50]
mDNS Querier	[DS] Kapitel "mDNS - Device/Service Discovery Protokoll" TA.mDNS.Querier	Das SMGW **MUSS+** an der HAN-CLS Schnittstelle mDNS Anfragen nach "cls.local." und "<CLS-ID>.local." senden und die empfangene CLS-ID, IP-Adresse und MAC-Adresse in die entsprechenden Datenfelder der ▸CLS-Statusliste übernehmen. [REQ.HKS.DNSDISCOVERY.10]
		Das SMGW **MUSS+** an der HAN-CLS-Schnittstelle als Antwort auf Anfragen von CLS empfangene DNS-SD TXT und SRV-Records der mDNS-Antworten in die entsprechenden Datenfelder von ▸Abschnitt 3.22.12 übernehmen. [REQ.HKS.DNSDISCOVERY.20]

Tabelle 4.21 Anforderungen an die Protokolllayer des HKS.DNSDISCOVERY

5 Nicht-Funktionale Anforderungen

5.1 Einleitung

Neben den funktionalen Anforderungen an ein SMGW, die in Kapitel ▸2.3 beschrieben wurden, existiert eine Reihe von nicht-funktionalen Anforderungen, die in den folgenden Kapiteln dargestellt werden.

5.2 Versiegelung

Das SMGW schützt sich gegen Angriffe, die einen lokalen Zugriff auf das SMGW voraussetzen. Bezüglich geltender Anforderungen wird hierbei auf [PP-0073] verwiesen. Technische Anforderungen an eine Versiegelung nach [MessEG]/[MessEV] werden im Rahmen dieser Technischen Richtlinie nicht thematisiert.

5.3 Eindeutige Geräte-Identifikation des SMGW

Das SMGW **MUSS** auf der Frontseite des Gehäuses eine ablesbare, alphanumerische, herstellerübergreifend-eindeutige Identifikationsnummer nach [DIN43849] mit der Spartenkennzeichnung "Kommunikation" besitzen, die der *SMGW-ID* entspricht. [REQ.WFA.SMGW-ID.10]

Das SMGW **MUSS** SM-PKI-Zertifikate besitzen, die auf diese SMGW-ID ausgestellt sind und den Subject Common Name gemäß [SM-PKI-CP] Anhang A enthalten. [REQ.WFA.SMGW-ID.20]

5.4 Einbau des Sicherheitsmoduls

Zur gegenseitigen Authentisierung zwischen SMGW und Sicherheitsmodul **MUSS** das SMGW das PACE-Verfahren verwenden [TR-03109-3]. [REQ.NFA.Einbau.10]

Die dafür benötigte PIN **MUSS** im SMGW geeignet geschützt werden. Der GWH **MUSS** diesen Mechanismus von einer CC-Prüfstelle sicherheitstechnisch begutachten lassen. [REQ.NFA.Einbau.20]

Hierbei **MUSS** die Prüfstelle für das sicherheitstechnische Gutachten analog zu der [CEM] nachweisen, dass das vorgeschlagene Verfahren zum Schutz der SMGW PIN resistent ist gegen das in [PP-0073] zugrunde gelegte Angriffspotential.

5.5 Vorhaltefristen

▸Tabelle 5.1 bestimmt die Dauer der Datenspeicherung im SMGW.

Das SMGW **MUSS** je Anschlussnutzer das Anschlussnutzer-Log gemäß ▸Tabelle 5.1 speichern können. [REQ.WFA.AnLog.20]

Das SMGW **MUSS** die Eichlog-Einträge gemäß ▸Tabelle 5.1 speichern können. [REQ.WFA.EichLog.10]

Das SMGW **MUSS** die Syslog-Einträge gemäß ▸Tabelle 5.1 speichern können. [REQ.WFA.SysLog.10]

Das SMGW **MUSS** die Vorhaltefristen gemäß ▸Tabelle 5.1 gewährleisten können. [REQ.NFA.ArchiveDuration.10]

Daten in SMGW	Mindestdauer der Vorhaltung
Vorhaltefristen gemäß [MessEG]/[MessEV]	
Registrierter Wert in ▸RWL	15 Monate ausgehend vom Datenfeld "Zeitstempel des Messwerts". Ein nachträglicher "On-Demand-Abruf" von Registrierten Werten ist auf 6 Wochen ausgehend vom Datenfeld "Zeitstempel des Messwertes" begrenzt.
Energiemengenregister in ▸AWL zum Ende der Abrechnungsperiode für ▸TAF2	15 Monate ausgehend vom Beginn der Abrechnungsperiode, deren Zählerstand als Teil der ▸AWL der Abrechnungsperiode gespeichert wird.
Lastgang ▸AWL für ▸TAF8	15 Monate ausgehend vom Datenfeld "Zeitstempel des Messwerts".
Energiemengenregister zur On-Demand-Auslesung für ▸TAF2	Ein nachträglicher "On-Demand-Abruf" von tagesscharfen Energiemengenregistern ist auf 6 Wochen ausgehend vom "Zeitstempel des Messwertes" begrenzt.

Daten in SMGW	Mindestdauer der Vorhaltung
▸RWL	Gemäß Vorhaltefrist der darin enthaltenen registrierten Werte. Eine Löschung ist erst möglich, wenn die Vorhaltefrist für alle enthaltenen registrierten Werte abgelaufen ist. Einzelne registrierte Werte, deren Vorhaltefrist bereits abgelaufen ist, dürfen gelöscht werden.
▸AWL	Gemäß Vorhaltefrist der darin enthaltenen abgeleiteten Werte. Eine Löschung ist erst möglich, wenn die Vorhaltefrist für alle enthaltenen abgeleiteten Werte abgelaufen ist. Einzelne abgeleitete Werte, deren Vorhaltefrist bereits abgelaufen ist, dürfen gelöscht werden.
Auswertungsprofil	Löschung möglich, sobald kein registrierter Wert und Tageswert der zugehörigen Messeinrichtung gemäß Auswertungsprofil mehr vorhanden ist.
Eichlog-Eintrag	36 Monate (1096 Tage) nach dem Schluss des Kalenderjahres, in dem der Eichlog-Eintrag erzeugt wurde ausgehend vom Zeitstempel des Log-Eintrags.
Anschlussnutzer-Log-Eintrag	Mindestens 15 Monate ausgehend vom Zeitstempel des Log-Eintrags, sofern den Anschlussnutzer im SMGW über die "userId" ein HAN-Kommunikationsprofil oder Auswertungsprofil zugeordnet ist.
Vorhaltefristen gemäß [MsbG]	
Tageswert	36 Monate (1096 Tage) ausgehend vom Datenfeld "Zeitstempel des Messwerts".
Tageswerteliste (TWL)	Gemäß Vorhaltefrist der darin enthaltenen Tageswerte. Eine Löschung ist erst möglich, wenn die Vorhaltefrist für alle enthaltenen Tageswerte abgelaufen ist. Einzelne Tageswerte, deren Vorhaltefrist bereits abgelaufen ist, dürfen gelöscht werden.
Technische Vorhaltefristen	
LMN-Kommunikationsprofil	Löschung möglich, sobald kein Auswertungsprofil mehr aktiv (d.h. innerhalb des Gültigkeitszeitraums) ist oder zukünftig aktiv wird (d.h. vor Beginn des Gültigkeitszeitraums), das über das Datenfeld ▸meterReadingInput.meterId (Zugeordnetes LMN-Kommunikationsprofil) auf das zu löschende LMN-Kommunikationsprofil verweist (referentielle Integrität).
EMT-WAN-Kommunikationsprofil	Löschung möglich, sobald kein Auswertungsprofil mehr aktiv (d.h. innerhalb des Gültigkeitszeitraums) ist oder zukünftig aktiv wird (d.h. vor Beginn des Gültigkeitszeitraums), welches über das Datenfeld ▸meterDataOutput.wanPeerRef (Zugeordnetes WAN-Kommunikationsprofil) auf das zu löschende WAN-Kommunikationsprofil verweist (referentielle Integrität).
Nicht-validierter Messwert	Ringspeicher über den konfigurierten rückwirkenden Zeitraum ausgehend vom Datenfeld "Zeitstempel des Messwertes". Die Konfiguration des Zeitraums erfolgt anhand der Versandperiode im zugehörigen Auswertungsprofil. Bei einem ungeplanten Neustart oder Spannungsverlust darf der Ringspeicher geleert werden, auch wenn die zuvor beschriebene Vorhaltefrist noch nicht abgelaufen ist.
Nicht-validierte Messwertliste (NWL)	Gemäß Vorhaltefrist der darin enthaltenen Messwerte. Eine Löschung ist erst möglich, wenn die Vorhaltefrist für alle enthaltenen Messwerte abgelaufen ist. Einzelne Messwerte, deren Vorhaltefrist bereits abgelaufen ist, dürfen gelöscht werden.
Syslog-Eintrag	Mindestens 1 Monat ausgehend vom Zeitstempel des Log-Eintrags und mindestens 10000 Einträge.

Tabelle 5.1 Vorhaltefristen

ICS

5.6 Mindestanforderungen an die Leistungsfähigkeit

Das SMGW **SOLL** mindestens von fünf Messeinrichtungen gleichzeitig Zählerstandsgänge mit 15-minütiger Registrierperiode (▸TAF7) gemäß der funktionalen Mindestanforderungen verarbeiten, und den ihnen zugeordneten verschiedenen Anschlussnutzern und EMT die Zählerstandsgänge für eine Gültigkeitsdauer der Auswertungsprofile von 15 Monaten unter Berücksichtigung der Vorhaltefristen gemäß ▸Abschnitt 5.5 bereitstellen können. [REQ.NFA.Performance.10]



ICS.NFA.Performance.20

Der GWH **MUSS** im ICS deklarieren, welche Anzahl von Messeinrichtungen das SMGW mindestens unterstützt, wenn die Anforderung ▸REQ.NFA.Performance.10 eingehalten wird.

5.7 Protokollierung IT-sicherheitsrelevanter Ereignisse

Gemäß [PP-0073] muss das SMGW IT-sicherheitsrelevante Ereignisse mit Audit-Funktionalität in Logs aufzeichnen.

Die IT-Sicherheitsrelevanten Ereignisse des System-Logs können vom GWA im Rahmen seiner Aufgaben (siehe [TR-03109-6]) für die Anomalieerkennung und zur Unterstützung von Systemen zur Angriffserkennung verwendet werden.

Nicht alle Ereignisse lassen sich in Bezug zu FAs oder Kommunikationsszenarien setzen. Um die Interoperabilität der Ereignisse zu verbessern, werden die Ereignisse den Audit-Anforderungen gemäß [CC] und [PP-0073] zugeordnet. Eine Event-SubId "0" identifiziert den Ausgang einer Funktion als erfolgreich ("Success"), eine Event-SubId größer "0" identifiziert den Ausgang einer Funktion als nicht erfolgreich.

Das SMGW **MUSS** die Ereignisse mit der Bedeutung gemäß ▸Tabelle 5.2 im Syslog protokollieren, sofern dies für ein SFR gemäß [PP-0073] gefordert wird. [REQ.NFA.AuditEvents.10]

Das SMGW **MUSS** die Ereignisse mit der Bedeutung gemäß ▸Tabelle 5.3 im UserLog protokollieren, sofern dies für ein SFR gemäß [PP-0073] gefordert wird. [REQ.NFA.AuditEvents.20] Sofern über ein Auswertungsprofil ein CLS (Identifiziert durch das HAN-Kommunikationsprofil zur "clsId") einem CON (Identifiziert durch das HAN-Kommunikationsprofil zur "userId") zugeordnet ist, werden die Audit-Events zum CLS in das User-Log (Anschlussnutzer-Log) für "userId" protokolliert.

Das SMGW **MUSS** die Ereignisse mit der Bedeutung und gemäß ▸Tabelle 5.4 im Eichlog protokollieren, sofern dies für ein SFR gemäß [PP-0073] gefordert wird. [REQ.NFA.AuditEvents.30]

Die folgenden Tabellen stellen den Bezug zwischen einer aus [PP-0073] und [CC] Part2 abgeleiteten Anforderung zur Protokollierung eines Ereignisses und einer nach dieser TR definierten, herstellerübergreifend einheitlichen, Ereignisidentifikation her.

Das SMGW kann weitere IT-sicherheitsrelevante Ereignisse für die SFRs protokollieren.



ICS.NFA.AuditEvents.10

Der GWH **MUSS** im ICS für die den SFRs zugeordneten Ereignisse jeweils die Ereignis-ID {vendor}.{eventId}.{eventSubId}, den Namen des Audit-Logs und den Grund des Ereignisses auflisten, sofern nicht eine konkrete Ereignis-ID für ein SFR gemäß ▸Tabelle 5.2, ▸Tabelle 5.3, ▸Tabelle 5.4 gefordert ist.

Übersicht der Audit-Ereignisse im Syslog

SFR	Audit Log Anforderung	Ereignis
Class FAU: Security Audit		
FAU_ARP.1/SYS	Actions taken due to potential security violations:	
	Anhaltende Störung der Sicherheitsfunktionalität des Sicherheitsmoduls. Betrieb wird eingestellt.	▸ [BSI.4010.2]
	IT-Sicherheitsanomalie des Sicherheitsmoduls erkannt. Betrieb wird fortgeführt.	▸ [BSI.4010.1]
	Zugriff auf Sicherheitsmodul wg. Authentifizierungsfehler abgelehnt	▸ [FNN.11002.1] ▸ [FNN.11002.2]
	Keine FW-Installation wegen fehlerhafter Firmware	▸ [BSI.18008.1] , ▸ [BSI.18008.2]
	Der Bootvorgang bzw. Startvorgang der Firmware wurde abgebrochen	▸ [FNN.19003.2] , ▸ [FNN.19004.1]
	Übergang in den operativen Betrieb trotz erkannter IT-Sicherheitsanomalie beim Bootvorgang	▸ [FNN.19003.1] , ▸ [FNN.19004.2]

SFR	Audit Log Anforderung	Ereignis
	Neustart der Komponente aufgrund einer IT-Sicherheitsverletzung	▸ [PTB.19002.1]
	Einstellung des operativen Betriebs aufgrund einer erkannten Integritätsverletzung	▸ [BSI.19001.1]
FAU_ARP.1/SYS Management	Management (addition, removal or modification) of actions	Kein FA zugeordnet.
FAU_GEN.1/SYS	Start/Stop des Syslog-Audits	▸ [BSI.19013.0] , ▸ [BSI.19013.1]
	Other non-privacy relevant auditable events	▸ICS.NFA.AuditEvents.10
FAU_GEN.1/CAL	Start/Stop des Eichlog-Audits	▸ [BSI.19014.0] , ▸ [BSI.19014.1]
FAU_GEN.1/ CON	Start/Stop des Userlog-Audits	▸ [BSI.19015.0] , ▸ [BSI.19015.1]
FAU_SAA.1/SYS	Enabling and disabling of any analysis mechanisms	▸ [BSI.19016.0] , ▸ [BSI.19016.1]
FAU_SAA.1/SYS Management	Maintenance of rules by (adding, modifying, deletion) of rules from set of rules.	Kein FA zugeordnet.
FAU_SAR.1/CAL	Reading of information from the audit records. Concerning the calibration log, every (read) access should be logged.	▸ [BSI.20036.0]
FAU_STG.5/CAL	Actions and warnings taken due to the audit storage failure. At least “Critical log capacity before overwriting 1st event” and “Capacity exhausted, initiating secure state” or similar.	▸ [BSI.19020.1]
FAU_STG.5/CAL Management	Maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure	Kein FA zugeordnet.
FAU_STG.5/CON FAU_STG.3	Actions and warnings taken due to the audit storage failure. At least “Critical Log Capacity before overwrite 1st value” and “1st value overwritten” or similar.	▸ [BSI.19018.1]
FAU_STG.5/CON Management	Maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.	Kein FA zugeordnet.
	Size configuration of the audit trail that is available before the oldest events get overwritten (as long as potential security violations can be detected).	▸ICS.NFA.AuditEvents.10
FAU_STG.5/SYS FAU_STG.3	Actions and warnings taken due to the audit storage failure. At least “Critical Log Capacity before overwrite 1st value” and “1st value overwritten” or similar.	▸ [BSI.19017.1]
FAU_STG.5/SYS Management	Maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.	Kein FA zugeordnet.
	Size configuration of the audit trail that is available before the oldest events get overwritten (as long as potential security violations can be detected).	▸ICS.NFA.AuditEvents.10
Class FCS: Cryptographic Support		
FCS_CKM.5 / CMAC, /X963	Failure of the specific activity. The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).	▸ICS.NFA.AuditEvents.10
FCS_CKM.5 / CMAC, /X963 Management	• Management of key material • Management of key material stored in the security module • Management of key material brought into the gateway during pairing process with meters	Kein FA zugeordnet
FCS_CKM.5 /TLS	Failure and the chosen cryptographic primitives.	▸ICS.NFA.AuditEvents.10

SFR	Audit Log Anforderung	Ereignis
FCS_CKM.5 /TLS Management	• Management of key material • Management of key material stored in the security module • Management of key material brought into the gateway during pairing process with meters	Erfolgs-Ereignisse zum Erzeugen von TLS-Schlüsselpaaren für die Schnittstellen des SMGW: Erfolgs-Ereignisse zum Import/Ändern/Löschen der TLS-Zertifikate in den WAN-/LMN/HAN-Kommunikationsprofilen Erfolgs-Ereignisse zum Erzeugen von TLS-Schlüsselpaaren und Zertifikaten für MTR und CLS.
FCS_CKM.1 / SERVICE	Failure of the specific activity. The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).	▸ICS.NFA.AuditEvents.10
FCS_CKM.1 / SERVICE Management	• Management of key material • Management of key material stored in the security module • Management of key material brought into the gateway during pairing process with meters	Erfolgs-Ereignisse zu **FA.DoCreateKeyPairAndClsCert, FA.DoInitialMtrSmgwPairing, FA.DoRenewMtrCertificate**
FCS_COP.1 / MEM, /HASH, / AESWRAP, / HMAC, / AESCMAC	Failure and the chosen cryptographic primitives.	▸ICS.NFA.AuditEvents.10
FCS_COP.1 / MEM Management	Management of key material.	Kein FA zugeordnet
FCS_COP.1 / AESWRAP, / HMAC, / AESCMAC Management	• Management of key material • Management of key material stored in the security module • Management of key material brought into the gateway during pairing process with meters	Kein FA zugeordnet
Class FDP: User Data Protection		
FDP_ACF.1	All requests to perform an operation on an object covered by the SFP.	▸ [BSI.19023.0]
FDP_IFF.1	All errors and warnings resulting on requests for information flow.	▸ICS.NFA.AuditEvents.10
FDP_IFF.1 Management	Managing the attributes used to make explicit access based decisions	Erfolgs-Ereignisse zu Management der Auswertungsprofile und Proxy-Kommunikationsprofile **FA.CreateProcessingProfile, FA.UpdateProcessingProfile, FA.DeleteProcessingProfile, FA.CreateProxyComProfile, FA.UpdateProxyComProfile, FA.DeleteProxyComProfile, FA.DoDeleteUserData, FA.DeleteArchivedProcessingProfile**
	Add authorized units for communication (pairing):	Erfolgs-Ereignisse zu **FA.DoInitialPairing** und **FA.CreateLmnComProfile**.
	Management of endpoint to be contacted after successful wake-up call	Ereignisse zur Erfolgreichen Änderung der Adresse oder der Zertifikate des GWA mittels **FA.CreateWanComProfile**, **FA.UpdateWanComProfile**, **FA.DeleteWanComProfile**,

SFR	Audit Log Anforderung	Ereignis
	Management of communication profiles:	Ereignisse zur erfolgreichen Änderung der Zertifikate und IDs in **FA.CreateLmnComProfile**, **FA.UpdateLmnComProfile**, **FA.DeleteLmnComProfile**, **FA.CreateHanUserProfile**, **FA.UpdateHanUserProfile**, **FA.DeleteHanUserProfile**,**FA.CreateWanComProfile**, **FA.UpdateWanComProfile**, **FA.DeleteWanComProfile**,**FA.DoDeleteUserData**
FDP_SDI.2	Failed attempts to check the integrity of user data.	▸ [BSI.15002.0] , ▸ [BSI.15001.0] , ▸ [BSI.15001.1]
Class FIA: Identification and Authentication		
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent, if appropriate, restoration to the normal state.	▸ICS.NFA.AuditEvents.10
FIA_AFL.1 Management	Management of the threshold for unsuccessful authentication attempts	Erfolgreiche Änderung des Datenfeldes "authAttemps" im HAN-Schnittstellenprofil durch **FA.UpdateHanIfProfile**
FIA_UAU.1, FIA_UAU.5, FIA_UID.1	Every authentication or identification attempt with result and corresponding user id where applicable	• LMN Successful: ▸ [FNN.1004.0] , ▸ [BSI.1005.0] • LMN Unsuccessful: ▸ [FNN.1004.1] , ▸ [FNN.1005.1] • HAN Successful: ▸ [FNN.5001.0] , ▸ [FNN.5002.0] , ▸ [FNN.5003.0] • HAN Unsuccessful: ▸ [FNN.5001.1] , ▸ [FNN.5002.1] ▸ [FNN.5003.1] • WAN Successful: ▸ [BSI.8001.0] , ▸ [BSI.9001.0] , ▸ [BSI.9003.0] , ▸ [BSI.9005.0] , ▸ [BSI.9007.0] • WAN Unsuccessful: ▸ [BSI.8001.1] , ▸ [BSI.9001.1] , ▸ [BSI.9003.1] , ▸ [BSI.9005.1] , ▸ [BSI.9007.1] • WAKEUP Successful: ▸ [BSI.7001.0] • WAKEUP Unsuccessful: ▸ [BSI.7001.4]
FIA_UID.1 Management	Management of the user identities	Erfolgs-Ereignisse zur TLS-Zertifikatsänderung , PSK-Änderung (LKS2) und User-Credentials (HKS.WS2) in **FA.CreateWanComProfile, FA.DeleteWanComProfile, FA.UpdateWanComProfile. FA.CreateHanUserProfile, FA.DeleteHanUserProfile, FA.UpdateHanUserProfile, FA.CreateLmnComProfile, FA.DeleteLmnComProfile, FA.UpdateLmnComProfile, FA.DoDeleteUserData,**
FIA_UAU.1 Management	Management of the authentication data by an authorized GWA	Erfolgs-Ereignisse zur TLS-Zertifikatsänderung , PSK-Änderung (LKS2) und User-Credentials (HKS.WS2) in **FA.CreateWanComProfile, FA.DeleteWanComProfile, FA.UpdateWanComProfile. FA.CreateHanUserProfile, FA.DeleteHanUserProfile, FA.UpdateHanUserProfile, FA.CreateLmnComProfile, FA.DeleteLmnComProfile, FA.UpdateLmnComProfile, FA.DoDeleteUserData,**
	Management of their own password as authentication data by the respective authorized consumer	Erfolgsereignis zu **FA.DoChangeUserPassword** ▸ [BSI.20033.0]

SFR	Audit Log Anforderung	Ereignis
FIA_USB.1	Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).	ICS.NFA.AuditEvents.10
Class FMT: Security Management		
FMT_MOF.1, FMT_SMF.1	Use of the management functions and corresponding user id. All modifications in the behaviour of the functions in the TSF and error messages in case of unallowed/undefined modification attempts.Only functions defined in FMT_SMF.1 should be executable. All further attempts should lead to an error message:	
	Veränderungen des (GWA-Event-)NotificationProfiles	Erfolgs-Ereignis zu **FA.UpdateNotificationProfile**: ICS.NFA.AuditEvents.10
	Management of profiles	Erfolgs-Ereignisse zu **FA.CreateWanComProfile, FA.DeleteWanComProfile, FA.UpdateWanComProfile. FA.CreateHanUserProfile, FA.DeleteHanUserProfile, FA.UpdateHanUserProfile, FA.CreateProxyComProfile, FA.DeleteProxyComProfile, FA.UpdateProxyComProfile, FA.CreateProcessingProfile, FA.DeleteProcessingProfile, FA.UpdateProcessingProfile, FA.DoDeleteUserData, FA.DeleteArchivedProcessingProfile.**
	Importieren von Root-CA-Zertifikaten	**FA.DoImportRootCaCert** [FNN.17009.0] , Import eines Zertifikates in das Sicherheitsmodul: [BSI.4009.0] ,
	Löschen von Root-CA-Zertifikaten	[FNN.17010.0]
	Importieren von SMGW-WAN-Zertifikaten	[FNN.17002.0]
	Erzeugen von SMGW-WAN-Schlüsselpaaren und WAN-CSRs	[FNN.17003.0]
	Erzeugen von SMGW-HAN-Schlüsselpaar und -Zertifikat	[FNN.17011.0]
	Löschen/Deaktivieren von SMGW-HAN-Schlüsselpaar und -Zertifikat	[FNN.17013.0]
	Erzeugen von SMGW-LMN-Schlüsselpaar und -Zertifikat	[FNN.17014.0]
	Löschen/Deaktivieren von SMGW-LMN-Schlüsselpaar und -Zertifikat	[FNN.17015.0]
	Ergänzen, Löschen, Aktualisieren von Sub-CA- und Endnutzer-Zertifikaten zur Authentisierung von Kommunikationspartnern	ICS.NFA.AuditEvents.10
	Anlegen, Löschen, Ändern von Schlüsselobjekten des Sicherheitsmodules (z.B. GWA-Schlüssel)	ICS.NFA.AuditEvents.10
	Pairing mit einer Messeinrichtung auslösen	ICS.NFA.AuditEvents.10
	Anlegen, Ändern, Löschen eines LMN- HAN- oder WAN-Kommunikationsprofiles (insbesondere der Identifikation des Kommunikationspartners, der Zertifikate und Credentials)	Anlegen: [FNN.20001.0] , Ändern: [BSI.20003.0] , Löschen: [FNN.20004.0] ICS.NFA.AuditEvents.10
	Ändern des Consumer-Passwortes	[BSI.20033.0]
	Neustart des SMGW auslösen	ICS.NFA.AuditEvents.10
	Firmware-Update des SMGW auslösen	[BSI.18001.0] , [BSI.18008.0]
	Selbsttest des SMGW auslösen	[BSI.15002.0]
	Schlüsselpaar- und Zertifikatserzeugung und -verteilung für Zähler auslösen	[BSI.1017.0]

SFR	Audit Log Anforderung	Ereignis
	Schlüsselpaar- und Zertifikatserzeugung und -verteilung für CLS auslösen	▸ [BSI.5004.0]
	Aufbau eines TLS-Proxykanals anfordern	▸ [FNN.20017.0]
	Reset-Funktion des SMGW auslösen (irreversible Nutzerdatenlöschung)	▸ [BSI.19019.0] , ▸ [BSI.19019.1]
	Anfordern einer Management-Verbindung durch GWA	▸ [BSI.7001.0]
	Ändern und Auslesen der WAN-Schnittstellenkonfiguration durch SRV	▸ICS.NFA.AuditEvents.10
FMT_MTD.1	All modifications of the values of TSF data: Delete audit data in the calibration audit trail	▸ [PTB.19012.0]
FMT_SMR.1 Management	Managing the group of users that are part of a role	Erfolgs-Ereignisse zu **FA.CreateWanComProfile**, **FA.DeleteWanComProfile**, **FA.CreateHanUserProfile**,.**FA.DeleteHanUserProfile**, **FA.CreateLmnComProfile**, **FA.DeleteLmnComProfile**
Class FPT: Protection of the TSF		
FPT_FLS.1	Failure of the TSF. • Deviation between local system time of the TOE and reliable external time source is too large • The calibration log is full • Other	• ▸ [PTB.13005.1] • ▸ [FNN.19008.2] • ▸ICS.NFA.AuditEvents.10
FPT_STM.1	Changes to the time: Stellen oder Synchronisieren der Zeit oder Zeitzone.	Erfolgs-Ereignisse zu **FA.TimeSyncWithGwa**: ▸ [PTB.13002.0] , ▸ [PTB.13003.0] , ▸ [FNN.13006.0] , ▸ [FNN.13007.0]
FPT_STM.1 Management	Management of a time source	Erfolgs-Ereignisse zu **FA.UpdateTimeSyncProfile** ▸ [BSI.13009.0]
FPT_STM.2	Changes to the time source	Erfolgs-Ereignisse zu **FA.UpdateTimeSyncProfile** ▸ [BSI.13009.0]
FPT_STM.2 Management	Management of a time source	Erfolgs-Ereignisse zu **FA.UpdateTimeSyncProfile**
FPT_TST.1	Trigger, execution and result of a selftest:	Alle Ereignisse zu **FA.DoSelfTest**: ▸ [BSI.15001.0] , ▸ [BSI.15001.1] , ▸ [BSI.15002.0]
Class FTP: Trusted Path/channels		
FTP_PRO.1/TLS12 FTP_PRO.1/TLS13	All attempted uses of the trusted channel, identification of the initiator and target of all trusted channel attempts:	Ereignisse zum TLS-Verbindungsaufbauversuch in WKS.MANAGEMENT, WKS.ADMIN-SERVICE, WKS.NTP-TLS, WKS.TLSPROXY, WKS.DOWNLOAD, LKS1, HKS.TLSPROXY.SOCKS, HKS.TLSPROXY.SRV, HKS.TLSPROXY.CLI, HKS.NTP-TLS.SRV, HKS.WS1, HKS.WS2: LKS1: ▸ [FNN.1004.0] , ▸ [FNN.1004.1]
FTP_PRO.2/TLS12 FTP_PRO.2/TLS13	All authentication attempts:	Erfolgreiche und nicht erfolgreiche TLS-Zertifikatsprüfung in WKS.MANAGEMENT, WKS.ADMIN-SERVICE, WKS.NTP-TLS, WKS.TLSPROXY, WKS.DOWNLOAD, LKS1, HKS.TLSPROXY.SRV, HKS.TLSPROXY.SOCKS, HKS.TLSPROXY.CLI, HKS.NTP-TLS.SRV, HKS.WS1, HKS.WS2 HKS: Unsuccessful requests/attempts: ▸ [FNN.5001.1] , ▸ [FNN.5002.1] ▸ [FNN.5003.1] LKS1 ▸ICS.NFA.AuditEvents.10 WKS: ▸ICS.NFA.AuditEvents.10

SFR	Audit Log Anforderung	Ereignis
FT-P_PRO.3/TLS12 FT-P_PRO.3/TLS13	Failures when attempting to verify channel properties in FTP_PRO.3.2/TLS12, FTP_PRO.3.2/TLS13.	▸ICS.NFA.AuditEvents.10
FTP_PRO.1/SYM	All attempted uses of the trusted channel, identification of the initiator and target of all trusted channel attempts. Not all functions transferred via the trusted channel must be logged	Initiieren eines LKS1.PSK Pairings und Empfangen von LKS2-Nachrichten (initial und ca. einmal täglich): ▸ICS.NFA.AuditEvents.10
FTP_PRO.2/SYM	All authentication attempts:	Erfolgreiche und nicht erfolgreiche Authentifizierung mit PSK in LKS1.PSK und LKS2: ▸ [BSI.1018.1]
FTP_PRO.3/SYM	Failures when attempting to verify channel properties in FTP_PRO.3.2/SYM.	▸ICS.NFA.AuditEvents.10
FTP_PRO.1/CMS	Failures when attempting to decrypt a CMS container.	WKS.MANAGEMENT, WKS.ADMIN-SERVICE, WKS.INFO-REPORT: ▸ [BSI.4004.1] , ▸ [BSI.4004.2]
FTP_PRO.3/CMS	Failures when attempting to validate the signature of a CMS container	WKS.MANAGEMENT: ▸ [BSI.4002.1] , ▸ [BSI.4002.2] , ▸ [BSI.4002.3]

Tabelle 5.2 Übersicht der Audit-Ereignisse im Syslog (Alphabetisch sortiert)

Übersicht der Audit-Ereignisse im Userlog

SFR	Audit Log Anforderung	Ereignis
Class FAU: Security Audit		
FAU_GEN.1/CON	Start-up of the audit functions;	▸ [BSI.19015.0]
	Shutdown of the audit functions;	▸ [BSI.19015.1]
	any change to a Processing Profile (The new and the old Processing Profile)	▸ [BSI.20010.0] (Anlegen), ▸ [PTB.20011.0] (Aktualisieren), ▸ [BSI.20013.0] (Löschen) eines Auswertungsprofils
	Any submission of Meter data that is not billing-relevant to an External Market Participant (The Processing Profile that lead to the submission in all cases the submission is not specified as periodical in the corresponding Processing)Profile (e.g. triggering by the GWA, or reaching a threshold)	▸ [BSI.16008.0]
	Any submission of billing-relevant data to an External Market Participant (The Processing Profile that lead to the submission. The submitted values)	▸ [BSI.16001.0]
	Any administrative action performed relevant to the specific user	Erfolgs-Ereignisse zu **FA.CreateHanComProfile, FA.UpdateHanComProfile, FA.DeleteHanComProfile, FA.CreateProcessingProfile, FA.UpdateProcessingProfile, FA.DeleteProcessingProfile, FA.CreateLmnComProfile, FA.DeleteLmnComProfile, FA.UpdateLmnComProfile** die mit der "userId" des Authentifizierten Nutzers und der "meterId" des Auswertungsprofiles verknüpft sind. ▸Tabelle 5.2 SFRs FMT_SMT.1 und FMT_MOF.1

SFR	Audit Log Anforderung	Ereignis
	Relevant system status information including relevant errors. This includes at least all events defined in ▸Tabelle 5.2 for • FAU_STG.5/CON, • FAU_STG.5/CAL, • FIA_AFL.1, • FPT_FLS.1, • FPT_STM.1, • FPT_STM.2, • FPT_TST.1	Siehe ▸Tabelle 5.2
Class FIA: Identification and Authentication		
FIA_AFL.1	Relevant system status information including relevant errors. In terms of FIA_AFL.1 only visible for the perpetrator of the failure, where applicable, and with a general entry in all other cases	▸[FNN.5001.1]
Class FPT: Protection of the TSF		
FPT_FLS.1	Failure of the TSF. • Deviation between local system time of the TOE and reliable external time source is too large • The calibration log is full • Other	• ▸[PTB.13005.1] • ▸[FNN.19008.2] • ▸ICS.NFA.AuditEvents.10
FPT_STM.1	Changes to the time	▸[PTB.13002.0] , ▸[PTB.13003.0] , ▸[FNN.13006.0] , ▸[FNN.13007.0]
FPT_STM.2	Changes to time source	▸[BSI.13009.0]
FPT_TST.1	Trigger, execution and result of a selftest.	▸[BSI.15001.0] , ▸[BSI.15001.1] , ▸[BSI.15002.0]

Tabelle 5.3 Übersicht der Audit-Ereignisse im Userlog (Alphabetisch sortiert)

Übersicht der Audit-Ereignisse im Eichlog

SFR	Audit Log Anforderung	Ereignis
Class FAU: Security Audit		
FAU_GEN.1/CAL	Start-up of the audit function	▸[BSI.19014.0]
	Shutdown of the audit functions	▸[BSI.19014.1]
	All events defined in ▸Tabelle 5.2 for • FAU_STG.5/CAL, • FDP_SDI.2, • FPT_FLS.1, • FPT_STM.1, • FPT_STM.2, • FPT_TST.1	Siehe ▸Tabelle 5.2
	all calibration-relevant information	▸ICS.NFA.AuditEvents.10
FAU_STG.5/CAL	For FAU_STG.5/CAL, this includes all actions taken due to the audit storage failure in the calibration log (after calibration log is available again).	▸[BSI.20036.0] Auslesen des Eichlogs
Class FPT: Protection of the TSF		

SFR	Audit Log Anforderung	Ereignis
FPT_FLS.1	Failure of the TSF. • Deviation between local system time of the TOE and reliable external time source is too large • The calibration log is full • Other	• ▸ [PTB.13005.1] • ▸ [FNN.19008.2] • ▸ICS.NFA.AuditEvents.10
FPT_STM.1	Changes to the time	▸ [PTB.13002.0] , ▸ [PTB.13003.0] , ▸ [FNN.13006.0] , ▸ [FNN.13007.0]
FPT_STM.2	Changes to time source	▸ [BSI.13009.0]
FPT_TST.1	Trigger, execution and result of a selftest.	▸ [BSI.15001.0] , ▸ [BSI.15001.1] , ▸ [BSI.15002.0]

Tabelle 5.4 Übersicht der Audit-Ereignisse im Eichlog (Alphabetisch sortiert)

Literaturverzeichnis

[CC] *Common Criteria for Information Technology Security Evaluation, CC:2022, Revision 1.* CCDB/ISO. September 2021.

[CEM] *Common Methodology for Information Technology Security Evaluation.* CCRA. November 2022.

[DIN43849] *DIN43849 (Ersetzt DIN 43863-5:2012-04) Messeinrichtungen und -systeme, sowie Zusatzeinrichtungen und Steuergeräte – Herstellerübergreifende Identifikationsnummer.* 2024. VDE|DKE K461.

[DS] *TR-03109-1 Detailspezifikationen.* Bundesamt für Sicherheit in der Informationstechnik. Aktuelle Fassung.

[DVGW-G685-4] *Gasabrechnung - Zählerstandsbasierte Energieermittlung.* DVGW. Dezember 2023.

[DVGW-G685-5] *Gasabrechnung - Lastgangbasierte Energieermittlung.* DVGW. August 2020.

[EEG] *Gesetz für den Ausbau erneuerbarer Energien (Erneuerbare Energien Gesetz - EEG).* Bundesministerium für Wirtschaft und Energie.

[EN13757-1] *DIN EN 13757-1 - Kommunikationssysteme für Zähler - Teil 1: Datenaustausch.* 2022. DIN/CEN TC294.

[EN13757-3] *DIN EN 13757-3 - Kommunikationssysteme für Zähler - Teil 3: Anwendungsprotokolle.* 2018. DIN/CEN TC294.

[EN13757-4] *DIN EN 13757-4 - Kommunikationssysteme für Zähler - Teil 4: Drahtlose M-Bus-Kommunikation.* 2019. DIN/CEN TC294.

[EN13757-7] *DIN EN 13757-7 - Kommunikationssysteme für Zähler - Teil 7: Transport- und Sicherheitsdienste.* 2018. DIN/CEN TC294.

[EN62056-6-1] *EN 62056-6-1: Electricity metering data exchange - The DLMS/COSEM suite - Part 6-1: Object Identification System (OBIS).* IEC TC13. 2017.

[EnWG] *Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz - EnWG).* Bundesministerium für Wirtschaft und Energie.

[IEEE 754] *IEEE Std 754-2019, Floating-Point Arithmetic.* IEEE. 22.07.2019.

[IEEE 802.3i] *IEEE Std 802.3 Clause 14, 10Base-T.* IEEE.

[IEEE 802.3u] *IEEE Std 802.3 Clause 24, 100Base-TX with Autonegotiation.* IEEE.

[ISO/IEC-Voc] *Standardization and related activities - General vocabulary.* ISO/IEC Guide 2:2004. 2004.

[MessEG] *Gesetz über das Inverkehrbringen und die Bereitstellung von Messgeräten auf dem Markt, ihre Verwendung und Eichung sowie über Fertigpackungen (Mess- und Eichgesetz - MessEG).* Bundesministerium für Wirtschaft und Energie.

[MessEV] *Verordnung über das Inverkehrbringen und die Bereitstellung von Messgeräten auf dem Markt sowie über ihre Verwendung und Eichung (Mess- und Eichverordnung - MessEV).* Bundesministerium für Wirtschaft und Energie.

[MsbG] *Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz - MsbG).* Bundesministerium für Wirtschaft und Energie.

[OMS-S2] *Open Metering System Specification - Volume 2 Primary Communication - Issue 5.0.1.* Dezember 2023. OMS-Group.

[PP-0073] *BSI-CC-PP-0073, Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP.* Bundesamt für Sicherheit in der Informationstechnik.

[PP-0077] *BSI-CC-PP-0077-2014, v1.3 Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP).* 2014. Bundesamt für Sicherheit in der Informationstechnik.

[RFC1918] *Address Allocation for Private Internets.* IETF. February 1996.

[RFC2119] *Key words for use in RFCs to Indicate Requirement Levels.* IETF und Scott Bradner. 1997.

[RFC3339] *Date and Time on the Internet: Timestamps.* IETF. July 2002.

[RFC3927] *Dynamic Configuration of IPv4 Link-Local Addresses.* IETF. Mai 2005.

[RFC3986] *Uniform Resource Identifier (URI): Generic Syntax.* IETF, Tim Berners-Lee, Roy T. Fielding und Larry Masinter. 2005.

[RFC4291] *IP Version 6 Addressing Architecture.* IETF. February 2006.

[RFC4648] *The Base16, Base32, and Base64 Data Encodings.* IETF. October 2006.

[RFC4862] *IPv6 Stateless Address Autoconfiguration.* IETF. September 2007.

[RFC5280] *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.* IETF, D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley und W. Polk. 2008.

[RFC5905] *Network Time Protocol Version 4: Protocol and Algorithms Specification.* IETF, D. Mills, J. Martin, J. Burbank und W. Kasch. 2010.

[RFC6763] *DNS-Based Service Discovery.* IETF. Februar 2013.

[RFC768] *User Datagram Protocol(UDP).* IETF. August 1980.

[RFC826] *An Ethernet Address Resolution Protocol.* IETF. November 1982.

[RFC9293] *Transmission Control Protocol (TCP).* IETF. August 2022.

[SM-PKI-CP] *SM-PKI-CP - Certificate Policy für die SM-PKI v1.1.2.* 2023. Bundesamt für Sicherheit in der Informationstechnik.

[SoZV] *Verordnung über die Einführung der mitteleuropäischen Sommerzeit ab dem Jahr 2002.* 2001.

[TR-03109-1-II] *Technische Richtlinie BSI-TR-03109-1, Anlage II: Webservice-APIs des SMGW.* 2024. Bundesamt für Sicherheit in der Informationstechnik.

[TR-03109-1-VI] *Technische Richtlinie BSI-TR-03109-1, Anlage VI: Betriebsprozesse, v2.0.* 2024. Bundesamt für Sicherheit in der Informationstechnik.

[TR-03109-1-VIII] Bundesamt für Sicherheit in der Informationstechnik. *Technische Richtlinie BSI-TR-03109-1, v2.0, Anlage VIII: Lebenszyklus.* 2024.

[TR-03109-2] *Technische Richtlinie BSI-TR-03109-2: Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls.* 2014. Bundesamt für Sicherheit in der Informationstechnik.

[TR-03109-3] *Technische Richtlinie BSI-TR-03109-3: Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen.* 2014. Bundesamt für Sicherheit in der Informationstechnik.

[TR-03109-4] *Technische Richtlinie BSI-TR-03109-4: Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways.* 2014. Bundesamt für Sicherheit in der Informationstechnik.

[TR-03109-5] *Technische Richtlinie TR-03109-5, v1.0: Kommunikationsadapter.* 2023. Bundesamt für Sicherheit in der Informationstechnik.

[TR-03109-6] *Technische Richtlinie BSI TR-03109-6: Smart Meter Gateway Administration.* 2015. Bundesamt für Sicherheit in der Informationstechnik.

[TR-03111] *Technical Guideline BSI-TR-03111: Elliptic Curve Cryptography.* 2018. Bundesamt für Sicherheit in der Informationstechnik.

[TR50572] *Functional reference architecture for communications in smart metering systems.* CEC/CLC/ETSI. 2011.

[VDE0418-63-7] *DIN VDE V 0418-63-7 (Bisher E DIN 43863-7): Messeinrichtungen und -systeme - Teil 63-7: Protokollstapel der leitungsgebundenen LMN-Schnittstelle.* VDE|DKE K461. 2023.

[VDE0418-63-8] *DIN VDE V 0418-63-8 (Bisher E DIN43863-8): Datenstrukturen der MSB/GWA-WAN-Schnittstelle des SMGW.* VDE|DKE K461. 2024.

[VDE0418-63-9] *DIN VDE 0418-63-9 (Bisher DIN43863-9): Messeinrichtungen und -systeme - Teil 63-9: Intelligentes Kommunikationsprotokoll für Elektrizitätszähler (SML).* VDE|DKE K461. 2022.

[VDE4400] *Messwesen Strom (Metering Code), VDE-AR-N-4400, VDE.* VDE. 2024.

[X.690] *ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).* 07/2002. ITU.

Glossar

Abrechnungsrelevanter Messwert	Ein mit einem geeichten und zertifizierten SMGW empfangener bzw. berechneter, gültiger und zeitgestempelter Zahlenwert einer *Messgröße* zuzüglich seiner Einheit zur Verwendung für die Abrechnung im geschäftlichen Verkehr.
Aktueller Wert	Als aktueller Wert wird der letzte, von einem Zähler übermittelte und im SMGW registrierte Messwert bezeichnet.
Auswertungsprofil	Ein Auswertungsprofil parametrisiert ein *Regelwerk*, für einen konkreten Anwendungsfall.
Normbedingungen	festgelegte Bedingungen, die verwendet werden, um das Gasvolumen unabhängig von den Messbedingungen (z. B. Temperatur: 273,15 K und absoluter Druck: 1,013 25 bar oder Temperatur: 288,15 K und absoluter Druck: 1,013 25 bar) anzugeben (Quelle: EB13757-1)
Bilanzierung	Bilanzkreisabrechnung gemäß Marktkommunikation.
CLS	Controllable Local System. Eine Komponente, die als TLS-Endpunkt über die logische Schnittstelle IF_GW_CLS mit dem SMGW kommuniziert
Eichtechnisches Log	Logbuch, in dem die nach [MessEG]/[MessEV] relevanten Ereignisse (z.B. erkannte Verfälschungen von Messungen, fehlgeschlagene Zeitsynchronisierungen) aufgezeichnet werden. Außerdem erfolgt hier die Registrierung von Änderungen an eichtechnisch relevanten Parametern (z.B. das Stellen der Geräteuhr). Dieses Log kann nur von dem autorisierten GWA eingesehen werden und wird bei Bedarf vom GWA den Eichbehörden zur Verfügung gestellt.
Stoff- oder Energiemenge	Menge an Elektrizität oder Gas, soweit sie zur leitungsgebundenen Energieversorgung und Energieeinspeisung verwendet werden. Bei Gas bezeichnet der Begriff das Gasvolumen.
Ereignis	(engl. event) Auftreten eines nachweisbaren oder feststellbaren Geschehens im Programmablauf des SMGW. Ereignisse können beispielsweise Fehler oder Zustandsänderungen sein. Im SMGW werden Ereignisse in den Kapiteln "Ereignisse" definiert.
Erzeugungsanlage	Anlage zur Erzeugung von Elektrizität, die an das Elektrizitätsversorgungsnetz angeschlossen ist oder für Gas.
Geräte-ID des Zählers	Der eindeutige Bezeichner des Zählers an dem der Anschlussnutzer 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 Anschlussnutzern oder Servicetechnikern fest.
kanonisierte Form	Zur Verarbeitung und zum Vergleich normalisierte Darstellung mit fester Länge, ohne Leerzeichen.
Kommunikationsprofil	Ein Oberbegriff für alle anderen Profile zur Festlegung von Parametern für die Kommunikation. Siehe *HAN-Kommunikationsprofil*, *WAN-Kommunikationsprofil* und *Proxy-Kommunikationsprofil*. Ein Kommunikationsprofil kann durch eine oder mehrere Datenstrukturen realisiert werden.

Kommunikationsszenario	Beschreibt die Komposition des Protokollstapels und die Datenflussrichtungen an einer Schnittstelle zwischen SMGW und einem weiteren Akteur.
Messeinrichtung	Siehe Zähler .
Messgröße	Physikalische Größe, deren Wert durch eine Messung bestimmt wird (z.B. Wirkleistung, Blindleistung, Spannung, Volumen).
Messart	Art, auf die eine Messwert bestimmt wird (z.B. Zeitintegral total, Zeitintegral über eine Periode, Momentanwert, Maximumwert).
Betriebsbedingungen	Zustandsbedingungen des Gases, dessen Volumen gemessen wird, am Messpunkt (z. B. die Temperatur und der Druck des Gases)
Messwert	Ein mit einem *Zähler* gemessener Zahlenwert einer *Messgröße* zuzüglich seiner Einheit.
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. In der technischen Umsetzung kann die Messwerteliste über eine *abgeleitete Werteliste* modelliert werden.
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.
OBIS-Kennzahl	Identifikation von Messwerten oder anderer abstrakter Daten.
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.
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.
Registrierperiode	Äquidistanter, mit der gesetzlichen Zeit synchroner Zeitraum zur Erfassung und Zeitstempelung von Messwerten.
Sollregistrierzeitpunkt	Zeitpunkt mit Datum und sekundengenauer Uhrzeit, dessen Uhrzeit ein Vielfaches einer *Registrierperiode* ab der Tageszeit 00:00:00 Uhr bei Elektrizität darstellt. Für eine *Registrierperiode* der Länge 15 Minuten bei Elektrizität: 00:15:00, 00:30:00, 00:45:00, ..., 00:00:00 des Folgetages. Messwerte werden im SMGW der jeweils gültigen Registrierperiode zugeordnet (registriert). Die Sollregistrierzeitpunkte bilden die Zeitbasis der registrierten Werteliste .
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.
TLS-Session	Die ausgehandelten Sicherheitsparameter und die TLS-Sitzungs-Schlüssel deren Lebensdauer die einer Verbindung zwischen Kommunikationspartnern überdauern können.
TLS-Verbindung	Eine über eine TLS-Session abgesicherte bidirektionale Transportverbindung zwischen zwei Kommunikationspartnern.

Verbrauch	Von einem Anschlussnutzer verbrauchte *Stoff- oder Energiemenge*.
WAN-Kommunikationsprofil	Ein WAN-Kommunikationsprofil legt die Parameter für die Kommunikation zu einem Kommunikationspartner im WAN fest. Der Begriff ist ein Hyperonym aus *EMT-Kommunikationsprofil* und *GWA-Kommunikationsprofil*.
EMT-Kommunikationsprofil	Ein Kommunikationsprofil legt die Parameter für die Kommunikation zu einem autorisierten EMT im WAN fest.
GWA-Kommunikationsprofil	Ein GWA-Kommunikationsprofil legt die Parameter für die Kommunikation zu einem autorisierten GWA im WAN fest.
Zähler	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.
SMGW-ID	Identifiziert das SMGW eindeutig in der SM-PKI und entspricht dem Namen des Inhabers der SMGW-Zertifikate (GW_WAN_SIG_CRT, GW_WAN_ENC_CRT, GW_WAN_TLS_CRT). Die "SMGW-ID" wird nach [SM-PKI-CP] Anhang A für das SMGW basierend auf der *kanonisierten Form* der herstellerübergreifend eindeutigen Messgeräteidentifikation nach [DIN43849] gebildet.
GWA_WAN_TLS_PUB	Der öffentliche Schlüssel des GWA für die TLS-Authentifizierung durch das SMGW als Octet-String nach [TR-03111] Kap 3.2.1.
GWA_WAN_AUT_PUB	Der öffentliche Schlüssel des GWA für die Authentifizierung des GWA am Sicherheitsmodul. Der Schlüssel ist identisch zu *GWA_WAN_TLS_PUB*.
SubjectCN	Das "commonName" Attribut des X.520 "distinguishedName" Attributes des "Subject"-Datenfeldes eines X.509-Zertifikates. Enthält den Namen des Zertifikatsinhabers.
SubjectDN	Das X.520 "distinguishedName" Attribut des "Subject"-Datenfeldes eines X.509-Zertifikates. Enthält die Namensattribute des Zertifikatsinhabers
IssuerDN	Das X.520 "distinguishedName" Attribut des "Issuer"-Datenfeldes eines X.509-Zertifikates. Enthält die Namensattribute des Zertifikatsausstellers.
GW_HAN_TLS_CRT	Das TLS-Authentifizierungszertifikat des SMGW an der HAN-Schnittstelle basierend auf [RFC5280] Kapitel 4.
SRV_HAN_TLS_CRT	Das TLS-Authentifizierungszertifikat des Servicetechnikers als HAN-Teilnehmer mit dem basierend auf [RFC5280] Kapitel 4
CON_HAN_TLS_CRT	Das TLS-Authentifizierungszertifikat des Anschlussnutzers (Consumer) als HAN-Teilnehmer basierend auf [RFC5280] Kapitel 4
CLS_HAN_TLS_CRT	Das TLS-Authentifizierungszertifikat eines CLS-Gerätes als HAN-Teilnehmer basierend auf [RFC5280] Kapitel 4

Anhang A Tabelle der zu protokollierenden Ereignisse

Die nachfolgende Tabelle enthält die zu protokollierenden Ereignisse für jede Anforderung der TR, die eine Protokollierung erfordert. Die Spalten der Tabelle haben dabei folgende Bedeutung:

- Die Spalte "Log-ID und Level" identifiziert die Art des zu protokollierenden Ereignisses eindeutig. Der Aufbau der Spalte entspricht "<vendor>.<eventid>.<eventsubid>".

  Der Level hat folgende Semantik (in der Reihenfolge zunehmender Schwere):

  - INFO: Information über die erfolgreiche Durchführung einer Aktion. Eine Intervention oder korrektive Maßnahme ist nicht notwendig. Ein solcher Logeintrag dient der Transparenz oder der Betriebsführung.
  - WARNING: Information über eine fehlgeschlagene Durchführung einer Aktion oder das Auftreten eines unerwarteten Zustands des SMGW (Anomalie). Die Aktion wird weiter durchgeführt. Eine Intervention oder korrektive Maßnahme ist derzeit nicht notwendig, jedoch kann zukünftig ein Ereignis mit einem höheren Level auf Basis derselben Ursache auftreten. Dieses Level wird auch für einige spezielle, erfolgreiche Aktionen verwendet, deren inkorrekte Verwendung negative Auswirkungen auf die Sicherheit oder die Einhaltung regulatorischer Rahmenbedingungen haben kann.
  - ERROR: Information über die fehlgeschlagene Durchführung einer Aktion oder das Auftreten eines unerwarteten Zustands des SMGW. Eine Intervention oder korrektive Maßnahme ist notwendig, um den weiteren Betrieb oder die korrekte Umsetzung einer Funktionalität sicherzustellen.
  - FATAL: Information über das Auftreten eines kritischen, nicht behebbaren Fehlers des SMGW.
- Die Spalte "Anforderung" benennt die Anforderung, zu der eine Protokollierung erfolgen soll.
- Die Spalte "Zeitpunkt / Ereignis" benennt den konkreten Zeitpunkt bzw. das konkrete Ereignis im Kontext der Anforderung, zu dem die Protokollierung erfolgen soll. Zu einer Anforderung können mehrere Zeitpunkte existieren, zu denen eine Protokollierung erfolgt.
- Die Spalte "Logs" benennt, in welche Logs das Ereignis protokolliert wird und ob eine Benachrichtigung des GWA erfolgt. Dabei sind nachfolgende Belegungen möglich. Ein Ereignis kann in mehrere Logs gleichzeitig protokolliert werden.
  - "SYS": das Ereignis wird im System-Log protokolliert.
  - "CAL": das Ereignis wird im Eichlog protokolliert.
  - "USER": das Ereignis wird im Anschlussnutzer-Log des oder der vom Ereignis betroffenen Anschlussnutzer protokolliert. Es findet keine Protokollierung in Anschlussnutzer-Logs unbeteiligter Anschlussnutzer statt. Welche Anschlussnutzer betroffen sind, ergibt sich aus dem Kontext der referenzierten Anforderung, beispielsweise aus der "userId" und "clsId" des Auswertungsprofils.
  - "ALLUSER": das Ereignis wird im Anschlussnutzer-Log aller parametrierten Anschlussnutzer protokolliert.
  - "NOTIFY": der GWA wird per Benachrichtigung über das Auftreten des Ereignisses informiert.

Zu einigen Ereignissen ist zusätzlich die Protokollierung weiterer Parameter erforderlich. Diese sind in den Folgezeilen des zugehörigen Ereignisses zusammen mit einem Datentyp und einer kurzen Beschreibung aufgezählt.

Log-ID	Anforderung			Zeitpunkt / Ereignis	Logs
FNN.20010.3 ERROR	▸REQ.FA.CreateProcessingProfile.10			Bei Ablehnung des Auswertungsprofils aufgrund des Fehlens mindestens eines referenzierten LMN-Kommunikationsprofils.	SYS
	[1]	name	meterId des nicht vorhandenen LMN-Kommunikationsprofils.		
FNN.20010.4 ERROR	▸REQ.FA.CreateProcessingProfile.30			Bei Ablehnung des Auswertungsprofils aufgrund des Fehlens mindestens eines referenzierten WAN-Kommunikationsprofils.	SYS
	[1]	name	Profil-ID des nicht vorhandenen WAN-Kommunikationsprofils.		

Log-ID	Anforderung			Zeitpunkt / Ereignis	Logs
FNN.20010.7 ERROR	▸REQ.FA.CreateProcessingProfile.15			Die Parameter im Auswertungsprofil sind nicht plausibel	SYS
	[1]	name	tafId des Auswertungsprofils		
	[2]	name	Der ungültige Parameter		
BSI.20010.0 INFO	▸REQ.WFA.EichlogInhalt.40 ▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.20 ▸REQ.NFA.AuditEvents.30			Das Auswertungsprofil wurde angelegt	SYS CAL USER
	[1]	name	Profil-ID des Auswertungsprofiles		
	[2]	name	tafType		
	[3]	name	Liste der verarbeiteten und abgeleiteten OBIS-IDs		
	[4]	name	Zähler-ID		
	[5]	name	userId		
	[6]	name	Gültigkeitszeitraum von		
	[7]	name	Gültigkeitszeitraum bis		
	[8]	name	Registrierperiode		
PTB.20011.0 INFO	▸REQ.WFA.EichlogInhalt.41 ▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.20 ▸REQ.NFA.AuditEvents.30			Das Auswertungsprofil wurde aktualisiert	SYS CAL USER
	[1]	name	Profil-ID des geänderten Auswertungsprofils.		
	[2]	String	Liste von Namen der Datenfelder mit Änderungen		
	[3]	String	Liste von Werten der Datenfelder vor Änderung		
	[4]	String	Liste von Werten der Datenfelder nach Änderung		
FNN.20011.6 ERROR	▸REQ.FA.UpdateProcessingProfile.20			Parameter ist schreibgeschützt	SYS CAL
	[1]	name	Profil-ID des geänderten Auswertungsprofils.		
	[2]	String	Liste von Namen veränderter, aber schreibgeschützter Parameter		
FNN.20011.5 ERROR	▸REQ.FA.UpdateProcessingProfile.15			Das Auswertungsprofil ist nicht plausibel	SYS
	[1]	name	Profil-ID des geänderten Auswertungsprofils.		
	[2]	name	Name des unplausiblen Parameters		
PTB.20032.0 INFO	▸REQ.FA.UpdateProcessingProfile.80			Das Enddatum des Gültigkeitszeitraumes wurde geändert	SYS CAL USER
	[1]	name	Profil-ID des geänderten Auswertungsprofils.		
	[2]	Date-Time	Neues Enddatum		
PTB.1011.2 ERROR	▸REQ.FAKAT.ValProcBilling.Registration.91			Bei erkanntem fatalen Fehler der Messeinrichtung.	SYS CAL USER NOTIFY
	[1]	name	Profil-ID des zur Messeinrichtung zugehörigen LMN-Kommunikationsprofils.		
	[2]	String	Von Messeinrichtung gemeldetes Statuswort.		
PTB.1012.1 ERROR	▸REQ.FAKAT.ValProcBilling.Registration.55			Bei erkanntem wiederholten Fehlen eines Messwerts.	SYS CAL NOTIFY
	[1]	name	Geräte-ID der Messeinrichtung.		

Log-ID	Anforderung			Zeitpunkt / Ereignis	Logs
PTB.13001.1 ERROR	▸REQ.WAF2.Zeitsynchronisation.52			Systemzeit wird als ungültig angenommen	SYS CAL ALLUSER NOTIFY
PTB.13001.2 ERROR	▸REQ.WAF2.Zeitsynchronisation.30			Gangreservezeit beim Systemstart überschritten	SYS CAL ALLUSER NOTIFY
	[1]	Date-Time	Letzte bekannte Systemzeit vor dem Ausfall		
PTB.13002.0 INFO	▸REQ.WAF2.Zeitsynchronisation.53 ▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.20 ▸REQ.NFA.AuditEvents.30			Systemzeit wurde gestellt	SYS CAL ALLUSER NOTIFY
	[1]	Date-Time	Zeitpunkt der gestellten Uhrzeit		
	[2]	Date-Time	Zeitpunkt der bisherigen Uhrzeit		
	[3]	Integer	Differenz in Millisekunden		
PTB.13002.1 ERROR	▸REQ.WAF2.Zeitsynchronisation.53			Systemzeit konnte nicht gestellt werden	SYS CAL ALLUSER
	[1]	String	Herstellerspezifischer Fehlercode		
PTB.13003.0 INFO	▸REQ.WAF2.Zeitsynchronisation.53 ▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.20 ▸REQ.NFA.AuditEvents.30			Synchronisation mit dem Zeitserver war erfolgreich	SYS CAL ALLUSER
	[1]	Date-Time	Zeitpunkt dieser Synchronisation		
	[2]	Date-Time	Zeitpunkt der vorherigen erfolgreichen Synchronisation		
	[3]	Integer	Bei der Synchronisation festgestellte Zeitabweichung in Millisekunden		
PTB.13003.1 ERROR	▸REQ.FA.SyncTimeWithGwa.10			Systemzeit konnte nicht synchronisiert werden	SYS
PTB.13004.1 WARNING	▸REQ.WAN.Zeitsynchronisation.100			Anhaltende Störung der Zeitsynchronisation	SYS NOTIFY
	[1]	Date-Time	Zeitpunkt der letzten erfolgreichen Synchronisation		
	[2]	Integer	Dauer (in Stunden) bis die Systemzeit als ungültig angenommen wird		
PTB.13004.2 ERROR	▸REQ.WAF2.Zeitsynchronisation.54			Dauerhafte Störung der Zeitsynchronisation, Zeit wird als ungültig angenommen.	SYS CAL ALLUSER NOTIFY
	[1]	Date-Time	Zeitpunkt der letzten erfolgreichen Synchronisation		
PTB.13005.1 ERROR	▸REQ.WAF2.Zeitsynchronisation.55 ▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.20 ▸REQ.NFA.AuditEvents.30			Fehlertoleranz (max. Zeitabweichung) überschritten.	SYS CAL ALLUSER
	[1]	Integer	gemessene Zeitabweichung in Millisekunden		
BSI.13008.1 ERROR	▸REQ.WAN.Zeitsynchronisation.80			Bei Überschreiten der max. RTT der Zeitsynchronisation.	SYS
	[1]	Integer	gemessene Round-Trip-Zeit zum GWA-Zeitserver		
	[2]	Integer	zulässige max. Round-Trip-Zeit zum GWA-Zeitserver		
	[3]	name	Profil-ID des WAN-Kommunikationsprofiles des GWA-Zeitservers		
FNN.17003.2 ERROR	▸REQ.FA.DoSmgwPkiCertRequest.10			Schlüsselpaare konnten im SecMod nicht erzeugt werden.	SYS

Log-ID	Anforderung			Zeitpunkt / Ereignis	Logs
	[1]	String	Herstellerspezifischer Fehlercode		
FNN.17003.0 INFO	▸REQ.FA.DoSmgwPkiCertRequest.50			Zertifikatsrequests erfolgreich erzeugt.	SYS
FNN.17003.1 ERROR	▸REQ.FA.DoSmgwPkiCertRequest.50			Zertifikatsrequests konnten nicht erzeugt werden.	SYS
	[1]	String	Herstellerspezifischer Fehlercode		
FNN.17002.1 ERROR	▸REQ.FA.DoImportSmgwPkiCerts.20			Mindestens ein Zertifikat ungültig.	SYS
	[1]	String	SubjectDN-Sequenznummer des SubCA-Zertifikates		
	[2]	String	SubjectDN-CommonName des SubCA-Zertifikates		
FNN.17002.2 ERROR	▸REQ.FA.DoImportSmgwPkiCerts.30			SMGW-WAN Zertifikate konnten nicht aktualisiert werden.	SYS
	[1]	String	SubjectDN-Sequenznummer des SMGW-Zertifikatstripels		
	[2]	String	IssuerDN-CommonName des SMGW-Zertifikatstripels		
	[3]	String	Herstellerspezifischer Fehlercode		
FNN.17002.0 INFO	▸REQ.FA.DoImportSmgwPkiCerts.30			SMGW-WAN Zertifikate erfolgreich aktualisiert.	SYS CAL ALLUSER
	[1]	String	SubjectDN-Sequenznummer des SMGW-Zertifikatstripels		
	[2]	String	IssuerDN-CommonName des SMGW-Zertifikatstripels		
FNN.17006.1 ERROR	▸REQ.FA.DoDeactivateSmgwPki-Certs.10			Löschen/Deaktivieren der SMGW-WAN-Schlüsselpaare und Zertifikate nicht möglich, da noch in Verwendung	SYS
	[1]	String	Identifiziert die Schlüsselbank		
	[2]	String	Herstellerspezifischer Fehlercode		
FNN.17006.0 INFO	▸REQ.FA.DoDeactivateSmgwPki-Certs.20			SMGW-WAN-Schlüsselpaare und Zertifikate gelöscht bzw. deaktiviert	SYS
	[1]	String	Identifiziert die Schlüsselbank		
BSI.17006.92 ERROR	▸REQ.FA.DoDeactivateSmgwPki-Certs.20			Löschen/Deaktivieren der SMGW-WAN-Schlüsselpaare und Zertifikate nicht möglich	SYS
	[1]	String	Identifiziert die Schlüsselbank		
	[2]	String	Herstellerspezifischer Fehlercode		
FNN.17009.0 INFO	▸REQ.FA.DoImportRootCaCert.60			RootCA-Zertifikat erfolgreich importiert	SYS
	[1]	String	SKI des Importierten Zertifikates		
FNN.17009.1 ERROR	▸REQ.FA.DoImportRootCaCert.60			RootCA-Zertifikat konnte nicht importiert werden	SYS
	[1]	String	SKI des Importierten Zertifikates		
	[2]	String	Herstellerspezifischer Fehlercode		
BSI.17009.2 ERROR	▸REQ.FA.DoImportRootCaCert.15			Ungültige/Unplausible Parameterdaten vom GWA	SYS
	[1]	String	SKI des Importierten Zertifikates		
	[2]	String	Herstellerspezifischer Fehlercode		
FNN.17010.2 ERROR	▸REQ.FA.DoDeactivateRootCaCert.10			RootCA Zertifikat nicht vorhanden	SYS
	[1]	String	SKI des zu deaktivierenden Zertifikates		
FNN.17010.1 ERROR	▸REQ.FA.DoDeactivateRootCaCert.20			RootCA Zertifikat konnte nicht deaktiviert werden	SYS
	[1]	String	Herstellerspezifischer Fehlercode		
FNN.17010.0 INFO	▸REQ.FA.DoDeactivateRootCaCert.30 ▸REQ.NFA.AuditEvents.10			RootCA Zertifikat wurde deaktiviert	SYS

Log-ID	Anforderung		Zeitpunkt / Ereignis	Logs
FNN.17014.0 INFO	▸REQ.FA.DoCreateSelfsignedSmgwLmnCert.30		Neues LMN-GW-Schlüsselpaar erzeugt	SYS
FNN.17014.1 ERROR	▸REQ.FA.DoCreateSelfsignedSmgwLmnCert.10		Es konnte kein neues LMN-GW-Schlüsselpaar erzeugt werden	SYS
	[1]	String	Herstellerspezifischer Fehlercode	
BSI.17014.92 ERROR	▸REQ.FA.DoCreateSelfsignedSmgwLmnCert.30		Es konnte kein neues LMN-GW-Schlüsselpaar erzeugt werden	SYS
	[1]	String	Herstellerspezifischer Fehlercode	
BSI.17014.93 ERROR	▸REQ.FA.DoCreateSelfsignedSmgwLmnCert.20		Aufrufparameter nicht unterstützt	SYS
	[1]	String	Bezeichner des Datenfeldes	
FNN.17011.0 INFO	▸REQ.FA.DoCreateSelfsignedSmgwHanCert.30 ▸REQ.NFA.AuditEvents.10		Neues HAN-GW-Schlüsselpaar erzeugt	SYS
FNN.17011.1 ERROR	▸REQ.FA.DoCreateSelfsignedSmgwHanCert.10		Es konnte kein neues HAN-GW-Schlüsselpaar erzeugt werden	SYS
	[1]	String	Herstellerspezifischer Fehlercode	
BSI.17011.92 ERROR	▸REQ.FA.DoCreateSelfsignedSmgwHanCert.30		Es konnte kein neues HAN-GW-Schlüsselpaar erzeugt werden	SYS
	[1]	String	Herstellerspezifischer Fehlercode	
BSI.17011.93 ERROR	▸REQ.FA.DoCreateSelfsignedSmgwHanCert.20		Aufrufparameter nicht unterstützt	SYS
	[1]	String	Bezeichner des Datenfeldes	
FNN.17015.1 ERROR	▸REQ.FA.DoDeactivateSelfsignedSmgwLmnCert.10		Das GW-LMN Schlüsselpaar konnte nicht gelöscht werden	SYS
	[1]	String	Herstellerspezifischer Fehlercode	
BSI.17015.92 ERROR	▸REQ.FA.DoDeactivateSelfsignedSmgwLmnCert.20		Das GW-LMN Schlüsselpaar konnte nicht gelöscht werden	SYS
	[1]	String	Herstellerspezifischer Fehlercode	
BSI.17015.93 ERROR	▸REQ.FA.DoDeactivateSelfsignedSmgwLmnCert.30		Das GW-LMN Schlüsselpaar konnte nicht gelöscht werden	SYS
	[1]	String	Herstellerspezifischer Fehlercode	
FNN.17015.0 INFO	▸REQ.FA.DoDeactivateSelfsignedSmgwLmnCert.30 ▸REQ.NFA.AuditEvents.10		Das GW-LMN Schlüsselpaar wurde gelöscht	SYS
	[1]	String	Herstellerspezifischer Fehlercode	
FNN.17013.1 ERROR	▸REQ.FA.DoDeactivateSelfsignedSmgwHanCert.10		Das GW-HAN Schlüsselpaar konnte nicht gelöscht werden	SYS
	[1]	String	Herstellerspezifischer Fehlercode	
FNN.17013.0 INFO	▸REQ.FA.DoDeactivateSelfsignedSmgwHanCert.30 ▸REQ.NFA.AuditEvents.10		Das GW-HAN Zertifikat wurde deaktiviert	SYS
	[1]	String	Herstellerspezifischer Fehlercode	
FNN.20005.3 ERROR	▸REQ.FA.CreateLmnComProfile.41		Profil ist nicht plausibel	SYS
	[1]	name	Geräte-ID aus dem Profil	
	[2]	String	Herstellerspezifischer Code	

Log-ID	Anforderung			Zeitpunkt / Ereignis	Logs
FNN.20005.4	▸REQ.FA.CreateLmnComProfile.40			Profil existiert bereits	SYS
ERROR	[1]	String	Geräte-ID aus dem Profil		
BSI.20005.0	▸REQ.FA.CreateLmnComProfile.50			Erfolgreich angelegt	SYS CAL
INFO	[1]	String	Geräte-ID aus dem Profil		
FNN.20006.3	▸REQ.FA.UpdateLmnComProfile.15			Profil ist nicht plausibel	SYS
ERROR	[1]	String	Geräte-ID aus dem Profil		
	[2]	String	Herstellerspezifischer Code		
FNN.20006.4	▸REQ.FA.UpdateLmnComProfile.16			Datenfeld kann nicht geändert werden	SYS
ERROR	[1]	String	Geräte-ID aus dem Profil		
	[2]	String	Name des Parameters		
BSI.20006.0	▸REQ.FA.UpdateLmnComProfile.30 ▸REQ.NFA.AuditEvents.10			Erfolgreich aktualisiert	SYS CAL
INFO	[1]	String	Geräte-ID aus dem Profil		
	[2]	String	Name des Parameters		
	[3]	String	Wert des Parameters		
FNN.20009.1	▸REQ.FA.DeleteLmnComProfile.10			Es existieren noch Referenzen auf das Profil	SYS
ERROR	[1]	String	Geräte-ID aus dem Profil		
	[2]	String	Referenz (Auswertungsprofil-ID)		
FNN.20009.0	▸REQ.FA.DeleteLmnComProfile.20 ▸REQ.NFA.AuditEvents.10			Erfolgreich gelöscht	SYS CAL
INFO	[1]	String	Geräte-ID aus dem Profil		
BSI.20030.0	▸REQ.FA.ReadLmnComProfile.10			LNN-Kommunikationsprofil erfolgreich ausgelesen	SYS
INFO	[1]	String	Geräte-ID aus dem Profil		
BSI.1010.2	▸REQ.FA.DoRemoveSmgwAssocIn-Mtr.10			Vorbedingungen für Crypto-Reset nicht erfüllt	SYS
ERROR	[1]	String	Identifikationsnummer der Messeinrichtung		
	[2]	String	Herstellerspezifischer Fehlergrund, warum der Crypto-Reset nicht durchgeführt werden kann		
FNN.1010.1	▸REQ.FA.DoRemoveSmgwAssocIn-Mtr.20			Zähler hat Crypto-Reset nicht bestätigt	SYS
ERROR	[1]	String	Identifikationsnummer der Messeinrichtung		
FNN.1010.0	▸REQ.FA.DoRemoveSmgwAssocIn-Mtr.20			Zähler hat Crypto-Reset bestätigt	SYS
INFO	[1]	String	Identifikationsnummer der Messeinrichtung		
FNN.17016.0	▸REQ.FA.DoExportSmgwLmnCert-ToMtr.10			SMGW-LMN-Schlüsselpaar aktualisiert	SYS CAL
INFO	[1]	String	Identifikationsnummer der Messeinrichtung		
FNN.17016.1	▸REQ.FA.DoExportSmgwLmnCert-ToMtr.10			SMGW-LMN-Schlüsselpaar nicht aktualisiert	SYS CAL
ERROR	[1]	String	Identifikationsnummer der Messeinrichtung		
FNN.20017.0	▸REQ.WAN.Kommunikationsszenarien.100 ▸REQ.NFA.AuditEvents.10			Aufbau eines CLS-Proxy Kanals angefordert	SYS
INFO					

Log-ID	Anforderung		Zeitpunkt / Ereignis	Logs
	[1]	String	Identifikation des Proxy-Kommunikationsprofiles	
FNN.20017.1 ERROR	▸REQ.WAN.Kommunikationsszenarien.100		Fehler beim Initiieren des CLS-Proxy-Kanals	SYS NOTIFY
	[1]	String	Identifikation des Proxy-Kommunikationsprofiles	
	[2]	String	Herstellerspezifische Fehlerbeschreibung	
BSI.20020.0 INFO	▸REQ.FA.CloseProxyCh.20		Erfolgreicher Abbau einer CLS-EMT-Verbindung	SYS NOTIFY
	[1]	String	Identifikation des Proxy-Kommunikationsprofiles	
FNN.20020.1 ERROR	▸REQ.FA.CloseProxyCh.20		CLS-EMT Verbindung wurde nicht abgebaut	SYS NOTIFY
	[1]	String	Identifikation des Proxy-Kommunikationsprofiles	
	[2]	String	Herstellerspezifische Fehlerbeschreibung	
BSI.20018.0 INFO	▸REQ.FA.RequestProxyChByCls.20 ▸REQ.FA.RequestProxyCh.50		Erfolgreicher Aufbau einer CLS-EMT-Verbindung	SYS NOTIFY
	[1]	String	Identifikation des Proxy-Kommunikationsprofiles	
FNN.20018.1 ERROR	▸REQ.FA.RequestProxyCh.40		CLS-EMT Verbindung wurde nicht aufgebaut (CLS Verbindungsproblem)	SYS NOTIFY
	[1]	String	Identifikation des Proxy-Kommunikationsprofiles	
	[2]	String	Herstellerspezifische Fehlerbeschreibung	
FNN.20018.2 ERROR	▸REQ.FA.RequestProxyChByCls.20 ▸REQ.FA.RequestProxyCh.50		CLS-EMT Verbindung wurde nicht aufgebaut (EMT Verbindungsproblem)	SYS NOTIFY
	[1]	String	Identifikation des Proxy-Kommunikationsprofiles	
	[2]	String	Herstellerspezifische Fehlerbeschreibung	
FNN.20019.0 INFO	▸REQ.FA.CloseProxyCh.20		CLS-Proxy Verbindung besteht nicht mehr (Erfolgreich abgebaut)	SYS
	[1]	String	Identifikation des Proxy-Kommunikationsprofiles	
FNN.20019.1 ERROR	▸REQ.FA.CloseProxyCh.20		CLS-Proxy Verbindung konnte nicht abgebaut werden (interner Fehler)	SYS
	[1]	String	Identifikation des Proxy-Kommunikationsprofiles	
	[2]	String	Herstellerspezifischer Fehler	
FNN.20016.1 ERROR	▸REQ.FA.DeleteProxyConfig.10		Proxy-Verbindung existiert noch	SYS
	[1]	String	Identifikation des Proxy-Kommunikationsprofiles	
FNN.20016.0 INFO	▸REQ.FA.DeleteProxyConfig.20		Proxy-Kommunikationsprofil erfolgreich gelöscht	SYS
	[1]	String	Identifikation des Proxy-Kommunikationsprofiles	
FNN.20015.6 ERROR	▸REQ.FA.UpdateProxyConfig.10		Proxy-Profil nicht plausibel	SYS
	[1]	String	Identifikation des Proxy-Kommunikationsprofiles	
	[2]	String	Name des Parameters	
FNN.20015.4 ERROR	▸REQ.FA.UpdateProxyConfig.20		Parameter ist schreibgeschützt	SYS
	[1]	String	Identifikation des Proxy-Kommunikationsprofiles	
	[2]	String	Name des Parameters	
FNN.20015.0 INFO	▸REQ.FA.UpdateProxyConfig.30		Proxy-Kommunikationsprofil erfolgreich aktualisiert	SYS
	[1]	String	Identifikation des Proxy-Kommunikationsprofiles	
FNN.20014.4 ERROR	▸REQ.FA.CreateProxyConfig.10		Proxy-Kommunikationsprofil existiert bereits	SYS
	[1]	String	Identifikation des Proxy-Kommunikationsprofiles	

Log-ID	Anforderung			Zeitpunkt / Ereignis	Logs
FNN.20014.2 ERROR	▸REQ.FA.CreateProxyConfig.15			Referenziertes WAN-Kommunikationsprofile existiert nicht	SYS
	[1]	String	Identifikation des Proxy-Kommunikationsprofiles		
FNN.20014.3 ERROR	▸REQ.FA.CreateProxyConfig.16			Referenziertes HAN-Kommunikationsprofile existiert nicht	SYS
	[1]	String	Identifikation des Proxy-Kommunikationsprofiles		
FNN.20014.5 ERROR	▸REQ.FA.CreateProxyConfig.20			Parameter im Proxy-Kommunikationsprofil sind nicht plausibel	SYS
	[1]	String	Identifikation des Proxy-Kommunikationsprofiles		
	[2]	String	Name des Parameters		
FNN.20014.0 INFO	▸REQ.FA.CreateProxyConfig.50			Proxy-Kommunikationsprofil erfolgreich angelegt	SYS
	[1]	String	Identifikation des Proxy-Kommunikationsprofiles		
FNN.17025.0 INFO	▸REQ.FA.DoPrepareSecmod.10			Die initialen Schlüsselbänke wurden aktiviert	SYS
FNN.17025.1 ERROR	▸REQ.FA.DoPrepareSecmod.10			Die initialen Schlüsselbänke konnten nicht aktiviert werden	SYS
	[1]	String	Herstellerspezifischer Fehlercode		
FNN.17023.0 INFO	▸REQ.FA.DoSwitchGwa.20			Neuer GWA wurde aktiviert und wird benachrichtigt	SYS NOTIFY
FNN.17023.1 ERROR	▸REQ.FA.DoSwitchGwa.30			Die Verbindung zum neuen GWA konnte nicht aufgebaut werden, der alte GWA bleibt aktiv	SYS NOTIFY
FNN.17024.1 ERROR	▸REQ.FA.DoDeactivateGwaCerts.10			Die GWA-Zertifikate konnten nicht deaktiviert werden	SYS
	[1]	Number	Nummer Schlüsselbank		
FNN.17024.0 INFO	▸REQ.FA.DoDeactivateGwaCerts.20			Die nicht mehr benötigten GWA-Zertifikate wurden deaktiviert	SYS
	[1]	Number	Nummer Schlüsselbank		
BSI.4009.1 ERROR	▸REQ.FA.DoImportGwaKeys.20			Das (CV-)Zertifikat mit der SubjectKeyID ist ungültig	SYS
	[1]	String	SubjecKeyID		
BSI.4009.2 ERROR	▸REQ.FA.DoImportGwaKeys.30			Beim Importieren des CV-Zertifikates mit der SubjectKeyID in das Sicherheitsmodul ist ein Fehler aufgetreten	SYS
	[1]	String	SubjecKeyID		
BSI.4009.0 INFO	▸REQ.FA.DoImportGwaKeys.30			Das Zertifikat mit der SubjectKeyID wurde importiert	SYS
	[1]	String	SubjecKeyID		
BSI.20031.0 INFO	▸REQ.FA.ReadWanComProfile.10 ▸REQ.FA.ReadProxyConfig.10			Kommunikationsprofil erfolgreich ausgelesen	SYS
	[1]	String	Profil-ID		
FNN.11001.0 INFO	▸REQ.FA.DoRequestSecmodAuth.10			AUTH Zustand wurde beantragt, Challenge gesendet	SYS
FNN.11001.1 ERROR	▸REQ.FA.DoRequestSecmodAuth.10			Fehler beim Erzeugen der Challenge	SYS
	[1]	String	Herstellerspezifischer Fehlergrund		
FNN.11002.0 INFO	▸REQ.FA.DoResponseSecmodAuth.20			AUTH Zustand wurde hergestellt	SYS

Log-ID	Anforderung			Zeitpunkt / Ereignis	Logs
FNN.11002.1 ERROR	▸REQ.FA.DoResponseSecmodAuth.20 ▸REQ.NFA.AuditEvents.10			AUTH Zustand wurde nicht hergestellt. Die Challenge wurde falsch beantwortet	SYS
FNN.11002.2 ERROR	▸REQ.FA.DoResponseSecmodAuth.55 ▸REQ.NFA.AuditEvents.10			AUTH Zustand wurde nicht hergestellt. Das Zertifikat im Aufrufparameter ist ungültig	SYS
	[1]	String	Seriennummer SN des Zertifikates im Aufrufparameter		
FNN.11001.2 ERROR	▸REQ.FA.DoRequestSecmodAuth.20			Das SMGW befindet sich bereits im AUTH Zustand	SYS
FNN.17017.0 INFO	▸REQ.FA.AcceptSwitchGwa.30			Der GWA-Wechsel wurde erfolgreich abgeschlossen, der neue GWA ist nun aktiv	SYS NOTIFY
FNN.11002.3 ERROR	▸REQ.FA.DoResponseSecmodAuth.50 ▸REQ.FA.DoResponseSecmodAuth.20			Der AUTH Zustand wurde nicht hergestellt. Es ist ein Fehler aufgetreten	SYS
	[1]	String	Herstellerspezifischer Fehlergrund		
BSI.7001.0 INFO	▸REQ.WAN.Kommunikationsszenarien.110 ▸REQ.NFA.AuditEvents.10			Empfang einer validen Wake-Up Nachricht	SYS
	[1]	String	Herstellerspezifische Bezeichnung der Schnittstelle, über die die Wake-Up Nachricht empfangen wurde		
FNN.7001.6 ERROR	▸REQ.WAN.WakeUpSicherung.30 ▸REQ.WAN.WakeUpSicherung.60			Ungewöhnliche Häufung von Wake-Up Nachrichten empfangen	SYS
	[1]	String	Herstellerspezifische Bezeichnung der Schnittstelle, über die die Wake-Up Nachricht empfangen wurde		
FNN.20004.1 ERROR	▸REQ.WAN.Kommunikationsprofil.60			Das Profil kann nicht gelöscht werden, da noch referentielle Abhängigkeiten bestehen	SYS
	[1]	String	Profil-Id		
BSI.20003.0 INFO	▸REQ.FA.UpdateWanComProfile.50 ▸REQ.FA.UpdateHanUserProfile.40 ▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.20			Profil erfolgreich aktualisiert	SYS USER
	[1]	String	Profil-Id		
FNN.20003.3 ERROR	▸REQ.FA.UpdateWanComProfile.30 ▸REQ.FA.UpdateHanUserProfile.20			Datenfeld darf nicht geändert werden	SYS
	[1]	String	Profil-Id		
	[2]	String	Parametername		
FNN.20003.2 ERROR	▸REQ.FA.UpdateHanUserProfile.10			Profil ist nicht plausibel	SYS
	[1]	String	Profil-Id		
	[2]	String	Parametername		
FNN.20001.0 INFO	▸REQ.FA.CreateWanComProfile.30 ▸REQ.FA.CreateHanUserProfile.40 ▸REQ.NFA.AuditEvents.10			Kommunikationsprofil erfolgreich angelegt	SYS USER
	[1]	String	Profil-Id		
	[2]	String	Name des Kommunikationsszenarios		

Log-ID	Anforderung			Zeitpunkt / Ereignis	Logs
FNN.20004.0 INFO	▸REQ.FA.DeleteWanComProfile.20 ▸REQ.FA.DeleteHanUserProfile.20 ▸REQ.NFA.AuditEvents.10			Kommunikationsprofil erfolgreich gelöscht	SYS
	[1]	String	Profil-Id		
	[2]	String	Liste der Zieladressen		
FNN.20001.3 ERROR	▸REQ.FA.CreateWanComProfile.50 ▸REQ.FA.CreateHanUserProfile.10			Kommunikationsprofil bereits vorhanden	SYS
	[1]	String	Profil-Id		
FNN.20001.2 ERROR	▸REQ.FA.CreateWanComProfile.20 ▸REQ.FA.CreateHanUserProfile.10			Kommunikationsprofil nicht plausibel	SYS
	[1]	String	Profil-Id		
	[2]	String	Gerätespezifische Fehlerbeschreibung		
BSI.18008.0 INFO	▸REQ.FA.DoFwActivation.5 ▸REQ.NFA.AuditEvents.10			Installation der Firmware gestartet	SYS
	[1]	String	Firmware-Paket Identifikation		
BSI.18008.1 ERROR	▸REQ.FA.DoFwActivation.20 ▸REQ.NFA.AuditEvents.10			Firmware nicht installiert. Firmware Authentizität oder Integrität nicht validierbar	SYS
	[1]	String	Firmware-Paket Identifikation		
BSI.18008.2 ERROR	▸REQ.FA.DoFwActivation.10 ▸REQ.NFA.AuditEvents.10			Firmware nicht installiert. Firmware nicht kompatibel mit Gerät	SYS CAL
	[1]	String	Firmware-Paket Identifikation		
	[2]	String	Firmware-Paket Version installiert		
	[3]	String	Firmware-Paket Version heruntergeladen		
BSI.18009.0 INFO	▸REQ.FA.DoFwActivation.50			Installation der Firmware im SMGW erfolgreich	SYS CAL NOTIFY
	[1]	String	Firmware-Paket Identifikation		
	[2]	String	Firmware-Paket Version bisher		
	[3]	String	Firmware-Paket Version aktuell		
BSI.18009.1 ERROR	▸REQ.FA.DoFwActivation.50			Installation der Firmware im SMGW fehlgeschlagen	SYS CAL NOTIFY
	[1]	String	Firmware-Paket Identifikation		
	[2]	String	Herstellerspezifischer Fehlercode		
BSI.18019.0 INFO	▸REQ.FA.DoFwActivation.50			Installation der Firmware in Messeinrichtung erfolgreich	SYS NOTIFY
	[1]	String	Geräte-ID der aktualisierten Messeinrichtung		
BSI.18019.1 ERROR	▸REQ.FA.DoFwActivation.50			Installation der Firmware in Messeinrichtung fehlgeschlagen	SYS NOTIFY
	[1]	String	Geräte-ID der zu aktualisierenden Messeinrichtung		
	[2]	String	Herstellerspezifischer Fehlercode		
BSI.18001.1 ERROR	▸REQ.FA.UpdateFwUpdateConfig.30 ▸REQ.FA.UpdateFwUpdateConfig.40			SMGW Firmware Updateanforderung kann nicht verarbeitet werden	SYS
	[1]	String	Firmware-Paket Identifikation		
	[2]	String	Herstellerspezifische Fehlerbeschreibung		

Log-ID	Anforderung			Zeitpunkt / Ereignis	Logs
BSI.18001.0 INFO	▸REQ.FA.UpdateFwUpdateConfig.20 ▸REQ.NFA.AuditEvents.10			SMGW Firmware Update angefordert	SYS
	[1]	String	Firmware-Paket Identifikation		
BSI.18002.0 INFO	▸REQ.FA.DoFwDownload.10			SMGW Firmware Download wurde gestartet	SYS CAL
	[1]	String	URL für den Download		
BSI.18003.1 WARNING	▸REQ.FA.DoFwDownload.40			SMGW Firmware Download wurde unterbrochen	SYS
	[1]	String	URL für den Download		
	[2]	String	Herstellerspezifische Fehlerbeschreibung		
BSI.18005.0 INFO	▸REQ.FA.DoFwDownload.50			SMGW Firmware Download wurde erfolgreich durchgeführt	SYS NOTIFY
	[1]	String	URL für den Download		
BSI.18002.1 ERROR	▸REQ.FA.DeleteFwUpdateConfig.20 ▸REQ.FA.DoFwDownload.40			SMGW Firmware Download wurde abgebrochen	SYS NOTIFY
	[1]	String	URL für den Download		
	[2]	String	Herstellerspezifische Fehlerbeschreibung		
BSI.15002.0 INFO	▸REQ.FA.DoSelftest.10 ▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.20 ▸REQ.NFA.AuditEvents.30			Selbsttest angefordert	SYS CAL ALLUSER
	[1]	String	Auslösender User		
	[2]	String	Zweck der Auslösung		
BSI.15001.0 INFO	▸REQ.WAN.Selbsttest.10 ▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.20 ▸REQ.NFA.AuditEvents.30			Selbsttest erfolgreich durchgeführt	SYS CAL ALLUSER NOTIFY
BSI.15001.1 ERROR	▸REQ.WAN.Selbsttest.10 ▸REQ.WAN.Selbsttest.20 ▸REQ.WAN.Selbsttest.21 ▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.20 ▸REQ.NFA.AuditEvents.30			Selbsttest fehlgeschlagen	SYS CAL ALLUSER NOTIFY
	[1]	Integer	Anzahl der Fehler		
	[2]	String	Liste der Fehler		
BSI.6006.0 INFO	▸REQ.WFA.SysLogInhalt.20			Betriebsspannungsausfall erkannt	SYS
	[1]	String	Datum und Uhrzeit des Beginns		
FNN.6005.0 INFO	▸REQ.FA.DoReboot.20			Erreichung administrative Betriebsbereitschaft	SYS
BSI.6001.0 INFO	▸REQ.WFA.SysLogInhalt.30			Betriebsspannungswiederkehr erkannt	SYS ALLUSER
	[1]	String	Datum und Uhrzeit der Wiederkehr		
FNN.17001.0 INFO	▸REQ.FA.NotifySystemEvents.10			Betriebsbereitschaft erreicht (SMGW Start)	SYS NOTIFY
	[1]	String	SMGW-ID		

Log-ID	Anforderung			Zeitpunkt / Ereignis	Logs
	[2]	String	WAN-IP Adresse		
FNN.2008.0 INFO	▸REQ.FA.NotifySystemEvents.10			WAN-IP-Adresse gewechselt	SYS NOTIFY
	[1]	String	SMGW-ID		
	[2]	String	WAN-IP Adresse		
BSI.8001.0 INFO	▸REQ.NFA.AuditEvents.10 ▸REQ.WKS.MANAGEMENT.60			MANAGEMENT-Kanal erfolgreich aufgebaut	SYS
	[1]	String	Identifikation des Kommunikationsprofiles		
BSI.2002.1 ERROR	▸REQ.WAN.Webservice.20			HTTP-Request mit Fehler (4xx, 5xx) beantwortet	SYS
	[1]	String	Typ (Method) der HTTP-Anfrage		
	[2]	String	URI der HTTP-Anfrage		
	[3]	String	Statuscode der HTTP-Response		
	[4]	String	Detailinformationen zur HTTP-Response		
FNN.2001.1 WARNING	▸REQ.WAN.Transport.51			Host nicht erreichbar	SYS
	[1]	String	IP-Adresse:Port des Hosts		
FNN.19006.0 INFO	▸REQ.WAF2.Zeitsynchronisation.60			Messbetrieb aufgenommen	SYS CAL ALLUSER NOTIFY
FNN.19008.1 WARNING	▸REQ.FAKAT.SmgwMonitoring.90			Verbleibender Speicherplatz für Eichlog ist 10% oder weniger	SYS CAL NOTIFY
	[1]	Number	Belegter Speicher für Eichlog in Prozent		
FNN.16004.0 INFO	▸REQ.FA.ExportNonAccntMtrReading.10 ▸REQ.FA.ExportAccntMtrReading.10			Bedarfsauslesung ausgelöst	SYS USER
	[1]	String	Datum der Bedarfsauslesung		
	[2]	String	Identifikation des Marktteilnehmers (SubjectCN)		
FNN.16004.4 WARNING	▸REQ.FA.DoOnDemandDelivery.60			Bedarfsauslesung ausgelöst	SYS CAL USER
	[1]	String	Datum der Bedarfsauslesung		
	[2]	String	Identifikation des Marktteilnehmers (SubjectCN)		
BSI.16001.0 INFO	▸REQ.FA.ExportAccntMtrReading.20 ▸REQ.FA.ExportNonAccntMtrReading.20 ▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.20			Messwertversand erfolgreich	SYS USER
	[1]	Number	Anzahl Messwerte		
	[2]	String	Zeitraum Start		
	[3]	String	Zeitraum Ende		
	[4]	String	Identifikation des Marktteilnehmers (SubjectCN)		
BSI.16001.1 ERROR	▸REQ.FA.ExportAccntMtrReading.20 ▸REQ.FA.ExportNonAccntMtrReading.20			Messwertversand nicht erfolgreich	SYS
	[1]	Number	Anzahl Messwerte		
	[2]	String	Zeitraum Start		

Log-ID	Anforderung			Zeitpunkt / Ereignis	Logs
	[3]	String	Zeitraum Ende		
	[4]	String	Identifikation des Marktteilnehmers (SubjectCN)		
BSI.16007.1 ERROR	▸REQ.FA.ExportNonAccntMtrReading.20			Versand von nicht-validierten Messwerten fehlgeschlagen	SYS USER
	[1]	Number	Anzahl fehlgeschlagener Versandversuche		
	[2]	String	Fehlerbeschreibung		
BSI.16008.1 ERROR	▸REQ.FA.ExportNonAccntMtrReading.20			Versand von Messwerten bei Schwellwertüberwachung fehlgeschlagen	SYS USER
	[1]	String	Fehlerbeschreibung		
BSI.16008.0 INFO	▸REQ.FA.ExportNonAccntMtrReading.10 ▸REQ.NFA.AuditEvents.20			Aperiodischer Versand von nicht-validierten Messwerten ausgelöst	SYS USER
	[1]	String	Identifikation des Auswertungsprofils		
BSI.16004.6 ERROR	▸REQ.FA.DoOnDemandDelivery.20			Auswertungsprofil nicht vorhanden	SYS
	[1]	String	Identifikation des Auswertungsprofils		
BSI.16004.7 ERROR	▸REQ.FA.DoOnDemandDelivery.10			Ungültiger Zeitpunkt für Abruf im Bedarfsfall	SYS
	[1]	String	Identifikation des Auswertungsprofils		
	[2]	String	Auslesezeitpunkt		
BSI.16004.8 ERROR	▸REQ.FA.DoOnDemandDelivery.80			Angabe eines Stichtags für diesen TAF unzulässig	SYS
	[1]	String	Identifikation des Auswertungsprofils		
BSI.9005.0 INFO	▸REQ.WKS.NTP-TLS.30 ▸REQ.NFA.AuditEvents.10			NTP-TLS-Kanal erfolgreich aufgebaut	SYS
	[1]	String	Identifikation des Kommunikationsprofiles		
BSI.1001.1 WARNING	▸REQ.LMN.LKS1.10			Der Zähler antwortet nicht auf den Broadcast 1	SYS
	[1]	hüid	Identifikation der Messeinrichtung		
FNN.1004.0 INFO	▸REQ.FAKAT.ValCapture.30 ▸REQ.NFA.AuditEvents.10			Die Kommunikation mit dem Zähler konnte erfolgreich hergestellt werden.	SYS NOTIFY
	[1]	hüid	Identifikation der Messeinrichtung		
FNN.1004.1 ERROR	▸REQ.LMN.LKS1.30 ▸REQ.NFA.AuditEvents.10			Die Kommunikation mit dem Zähler konnte nicht hergestellt werden.	SYS NOTIFY
	[1]	hüid	Identifikation der Messeinrichtung		
BSI.1005.0 INFO	▸REQ.LMN.LKS1.PSK.30 ▸REQ.NFA.AuditEvents.10			Das Pairing mit dem Zähler wurde erfolgreich durchgeführt.	SYS CAL NOTIFY
	[1]	hüid	Identifikation der Messeinrichtung		
FNN.1005.1 ERROR	▸REQ.LMN.LKS1.PSK.30			Das Pairing mit dem Zähler konnte nicht durch durchgeführt werden. Eine Wiederholung ist möglich.	SYS NOTIFY
	[1]	hüid	Identifikation der Messeinrichtung		
FNN.1005.2 ERROR	▸REQ.LMN.LKS1.PSK.30			Das Pairing mit dem Zähler konnte nicht durch durchgeführt werden. Eine Wiederholung ist nicht möglich	SYS NOTIFY
	[1]	hüid	Identifikation der Messeinrichtung		
	[2]	String	Herstellerspezifischer Fehler		
BSI.1009.1 ERROR	▸REQ.LMN.Kommunikationsprotokolle.50			Verarbeitung der SML-Nachricht des Zählers fehlgeschlagen	SYS NOTIFY

Log-ID	Anforderung			Zeitpunkt / Ereignis	Logs
	[1]	String	Identifikation der Messeinrichtung		
BSI.1006.1 WARNING	▸REQ.LMN.Kommunikationsprotokolle.50			SML-GET Anfrage mit OBIS-ID wurde mit unerwarteter SML-Attention beantwortet	SYS
	[1]	String	OBIS-ID		
	[2]	String	Identifikation der Messeinrichtung		
FNN.1014.1 WARNING	▸REQ.LMN.Kommunikationsprotokolle.50			Der Zähler antwortet nicht auf SML Anfragen im erwarteten Zeitbereich	SYS NOTIFY
	[1]	Number	Dauer der Zeitüberschreitung		
PTB.19012.0 INFO	▸REQ.FA.DoTruncateCalLog.20			Eichlog wurde verkürzt	SYS CAL ALLUSER
	[1]	String	GWA-ID des authentifizierten GWA		
	[2]	Integer	Anzahl gelöschter Einträge		
	[3]	Integer	Fortlaufende Nummer des ersten/ältesten gelöschten Eintrages		
	[4]	Integer	Fortlaufende Nummer des letzten/jüngsten gelöschten Eintrages		
BSI.19012.1 ERROR	▸REQ.FA.DoTruncateCalLog.10			Eichlog nicht verkürzt, da Datum nicht zulässig	SYS CAL
	[1]	String	GWA-ID des authentifizierten GWA		
	[2]	Date-Time	Datum das zum Fehler führte		
BSI.20013.0 INFO	▸REQ.FA.DeleteProcessingProfile.30 ▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.20 ▸REQ.NFA.AuditEvents.30			Das Auswertungsprofil wurde gelöscht	SYS CAL USER
	[1]	name	Profil-ID des gelöschten Auswertungsprofils.		
FNN.20013.1 ERROR	▸REQ.FA.DeleteProcessingProfile.20			Nicht gelöscht, da Archivierungsdauer noch nicht erreicht	SYS
	[1]	name	Profil-ID des zu löschenden Auswertungsprofils.		
	[2]	Number	Restliche Archivierungsdauer (in Tagen) des zu löschenden Auswertungsprofils.		
FNN.20013.3 ERROR	▸REQ.FA.DeleteProcessingProfile.10			Das Auswerteprofil kann noch nicht gelöscht werden, da die Endablesung noch nicht durchgeführt wurde.	SYS
	[1]	name	Profil-ID des zu löschenden Auswertungsprofils.		
BSI.4001.1 ERROR	▸REQ.WKS.MANAGEMENT.40			Die Struktur des CMS-Containers ist ungültig	SYS NOTIFY
BSI.4002.1 ERROR	▸REQ.WAN.CmsSicherung.30			Die Signatur zu dem Zertifikat konnte nicht validiert werden (Signatur nicht übereinstimmend).	SYS NOTIFY
	[1]	name	SubjectKeyId des Signatur-Zertifikates im CMS-Container		
BSI.4002.2 ERROR	▸REQ.WAN.CmsSicherung.30			Die Signatur zu dem Zertifikat konnte nicht validiert werden (Zertifikat ungültig).	SYS
	[1]	name	SubjectKeyId des Signatur-Zertifikates im CMS-Container		
BSI.4002.3 ERROR	▸REQ.WAN.CmsSicherung.30			Die Signatur zu dem Zertifikat konnte nicht validiert werden (Sonstiger Fehler).	SYS
	[1]	name	SubjectKeyId des Signatur-Zertifikates im CMS-Container		
	[2]	name	Herstellerspezifischer Fehlergrund		
BSI.4004.1 ERROR	▸REQ.WAN.CmsSicherung.31			Inhaltsdaten konnten nicht entschlüsselt werden (Zertifikat ungültig).	SYS
	[1]	name	SubjectKeyId des Verschlüsselungs-Zertifikates im CMS-Container		

Log-ID	Anforderung			Zeitpunkt / Ereignis	Logs
BSI.4004.2 ERROR	▸REQ.WAN.CmsSicherung.31			Inhaltsdaten konnten nicht entschlüsselt werden (Sonstiger Fehler).	SYS
	[1]	name	SubjectKeyId des Verschlüsselungs-Zertifikates im CMS-Container		
	[2]	name	Herstellerspezifischer Fehlergrund		
BSI.30002.8 ERROR	▸REQ.WAN.TlsSicherung.40			Der Typ des im TLS-Handshakes empfangenen Zertifikates wird nicht unterstützt.	SYS
	[1]	name	SubjectKeyId des im Handshake empfangenen TLS--Zertifikates		
BSI.9003.0 INFO	▸REQ.WKS.INFO-REPORT.50			INFO-REPORT-Kanal erfolgreich aufgebaut	SYS
	[1]	String	Identifikation des Kommunikationsprofiles		
BSI.9003.1 ERROR	▸REQ.WKS.INFO-REPORT.50 ▸REQ.NFA.AuditEvents.10			INFO-REPORT-Kanal konnte nicht aufgebaut werden	SYS
	[1]	String	Identifikation des Kommunikationsprofiles		
BSI.8001.1 ERROR	▸REQ.WKS.MANAGEMENT.60			MANAGEMENT-Kanal konnte nicht aufgebaut werden	SYS
	[1]	String	Identifikation des Kommunikationsprofiles		
BSI.9001.0 INFO	▸REQ.WKS.ADMIN-SERVICE.50 ▸REQ.WKS.INFO-REPORT.51 ▸REQ.NFA.AuditEvents.10			ADMIN-SERVICE-Kanal erfolgreich aufgebaut	SYS
	[1]	String	Identifikation des Kommunikationsprofiles		
BSI.9001.1 ERROR	▸REQ.WKS.ADMIN-SERVICE.50 ▸REQ.WKS.INFO-REPORT.51			ADMIN-SERVICE-Kanal konnte nicht aufgebaut werden	SYS
	[1]	String	Identifikation des Kommunikationsprofiles		
BSI.9005.1 ERROR	▸REQ.WKS.NTP-TLS.30 ▸REQ.NFA.AuditEvents.10			NTP-TLS-Kanal konnte nicht aufgebaut werden	SYS
	[1]	String	Identifikation des Kommunikationsprofiles		
BSI.9007.0 INFO	▸REQ.WKS.DOWNLOAD.30			DOWNLOAD-Kanal erfolgreich aufgebaut	SYS
	[1]	String	Identifikation des Kommunikationsprofiles		
BSI.9007.1 ERROR	▸REQ.WKS.DOWNLOAD.30 ▸REQ.NFA.AuditEvents.10			DOWNLOAD-Kanal konnte nicht aufgebaut werden	SYS
	[1]	String	Identifikation des Kommunikationsprofiles		
BSI.8002.0 INFO	▸REQ.WAN.Transport.80			MANAGEMENT-Kanal wurde erfolgreich abgebaut	SYS
	[1]	String	Identifikation des Kommunikationsprofiles		
BSI.8002.1 ERROR	▸REQ.WAN.Transport.80			MANAGEMENT-Kanal konnte nicht abgebaut werden	SYS
	[1]	String	Identifikation des Kommunikationsprofiles		
BSI.9002.0 INFO	▸REQ.WAN.Transport.80			ADMIN-SERVICE-Kanal wurde erfolgreich abgebaut	SYS
	[1]	String	Identifikation des Kommunikationsprofiles		
BSI.9002.1 ERROR	▸REQ.WAN.Transport.80			ADMIN-SERVICE-Kanal konnte nicht abgebaut werden	SYS
	[1]	String	Identifikation des Kommunikationsprofiles		
BSI.9004.0 INFO	▸REQ.WAN.Transport.80			INFO-REPORT-Kanal wurde erfolgreich abgebaut	SYS
	[1]	String	Identifikation des Kommunikationsprofiles		
BSI.9004.1 ERROR	▸REQ.WAN.Transport.80			INFO-REPORT-Kanal konnte nicht abgebaut werden	SYS
	[1]	String	Identifikation des Kommunikationsprofiles		

Log-ID	Anforderung			Zeitpunkt / Ereignis	Logs
BSI.9006.0 INFO	▸REQ.WAN.Transport.80			NTP-TLS-Kanal wurde erfolgreich abgebaut	SYS
	[1]	String	Identifikation des Kommunikationsprofiles		
BSI.9006.1 ERROR	▸REQ.WAN.Transport.80			NTP-TLS-Kanal konnte nicht abgebaut werden	SYS
	[1]	String	Identifikation des Kommunikationsprofiles		
BSI.9008.0 INFO	▸REQ.WAN.Transport.80			DOWNLOAD-Kanal wurde erfolgreich abgebaut	SYS
	[1]	String	Identifikation des Kommunikationsprofiles		
BSI.9008.1 ERROR	▸REQ.WAN.Transport.80			DOWNLOAD-Kanal konnte nicht abgebaut werden	SYS
	[1]	String	Identifikation des Kommunikationsprofiles		
BSI.2003.1 WARNING	▸REQ.WKS.ADMIN-SERVICE.80 ▸REQ.WKS.INFO-REPORT.50			Zu einem gesendeten HTTP-Request wurde keine Antwort empfangen	SYS
	[1]	String	Verb/Typ		
	[2]	String	URI		
BSI.2003.2 WARNING	▸REQ.WKS.ADMIN-SERVICE.100 ▸REQ.WKS.DOWNLOAD.80 ▸REQ.WKS.INFO-REPORT.70			Ein gesendeter HTTP-Request wurde von der Gegenstelle mit Fehlerstatus beantwortet	SYS
	[1]	String	Verb/Typ		
	[2]	String	URI		
	[3]	Integer	Statuscode		
BSI.2003.0 INFO	▸REQ.WKS.ADMIN-SERVICE.100 ▸REQ.WKS.DOWNLOAD.80 ▸REQ.WKS.INFO-REPORT.70			Ein gesendeter HTTP-Request wurde positiv von der Gegenstelle beantwortet	SYS
	[1]	String	Verb/Typ		
	[2]	String	URI		
	[3]	Integer	Statuscode		
BSI.18011.0 INFO	▸REQ.FA.DoFwActivation.50			Installation der Firmware in der Messeinrichtung erfolgreich	SYS CAL USER NOTIFY
	[1]	String	Firmware-Paket Identifikation		
	[2]	hüid	Identifikation der Messeinrichtung		
BSI.18011.1 ERROR	▸REQ.FA.DoFwActivation.50			Installation der Firmware in der Messeinrichtung fehlgeschlagen	SYS CAL USER NOTIFY
	[1]	String	Firmware-Paket Identifikation		
	[2]	hüid	Identifikation der Messeinrichtung		
	[3]	String	Fehlergrund		
BSI.1016.0 INFO	▸REQ.FA.ExportFileToMtr.20			Datei wurde erfolgreich an die Messeinrichtung übermittelt	SYS CAL
	[1]	hüid	Identifikation der Messeinrichtung		
	[2]	name	Typ der Datei (z.B. OBIS-ID)		
BSI.1016.1 ERROR	▸REQ.FA.ExportFileToMtr.20			Datei konnte nicht an die Messeinrichtung übermittelt werden	SYS CAL
	[1]	hüid	Identifikation der Messeinrichtung		
	[2]	name	Typ der Datei (z.B. OBIS-ID)		
	[3]	String	Fehlergrund		

Log-ID	Anforderung			Zeitpunkt / Ereignis	Logs
BSI.1017.0 INFO	▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.30 ▸REQ.LMN.TlsSicherung.70 ▸REQ.FA.DoInitialMtrSmgwPairing.30			Neues Schlüsselpaar und Zertifikat für die Messeinrichtung erfolgreich erzeugt und übermittelt	SYS CAL
	[1]	hüid	Identifikation der Messeinrichtung		
BSI.1017.1 ERROR	▸REQ.NFA.AuditEvents.10 ▸REQ.LMN.TlsSicherung.70 ▸REQ.FA.DoInitialMtrSmgwPairing.30			Fehler beim Erzeugen eines Schlüsselpaares/Zertifikates für die Messeinrichtung	SYS
	[1]	hüid	Identifikation der Messeinrichtung		
	[2]	String	Fehlerbeschreibung		
BSI.1017.2 ERROR	▸REQ.NFA.AuditEvents.10 ▸REQ.FA.DoRenewMtrCertificate.10 ▸REQ.FA.DoInitialMtrSmgwPairing.30			Fehler beim Übertragen des Schlüsselpaares/Zertifikates an die Messeinrichtung	SYS
	[1]	hüid	Identifikation der Messeinrichtung		
	[2]	String	Fehlerbeschreibung		
BSI.5004.0 INFO	▸REQ.NFA.AuditEvents.10 ▸REQ.FA.DoCreateKeyPairAndClsCert.40			Neues Schlüsselpaar und Zertifikat für CLS erfolgreich erzeugt und übermittelt	SYS
	[1]	hüid	Identifikation der Messeinrichtung		
BSI.5004.1 ERROR	▸REQ.NFA.AuditEvents.10 ▸REQ.FA.DoCreateKeyPairAndClsCert.30			Fehler beim Erzeugen eines Schlüsselpaares/Zertifikates für CLS	SYS
	[1]	name	Identifikation des CLS/Profils		
	[2]	String	Fehlerbeschreibung		
BSI.5004.2 ERROR	▸REQ.NFA.AuditEvents.10 ▸REQ.FA.DoCreateKeyPairAndClsCert.40			Fehler beim Übertragen des Schlüsselpaares/Zertifikates an das CLS	SYS
	[1]	name	Identifikation des CLS/Profils		
	[2]	String	Fehlerbeschreibung		
FNN.5002.0 INFO	▸REQ.HAN.HKS1.60 ▸REQ.NFA.AuditEvents.10			Anmeldung mit einem Benutzerzertifikat erfolgreich	SYS USER
	[1]	name	Subject-DN des Zertifikates		
	[2]	name	Issuer-DN des Zertifikates		
FNN.5002.1 WARNING	▸REQ.HAN.HKS1.20 ▸REQ.NFA.AuditEvents.10			Anmeldung mit einem Benutzerzertifikat fehlgeschlagen	SYS
	[1]	name	Subject-DN des Zertifikates		
	[2]	name	Issuer-DN des Zertifikates		
FNN.5001.0 INFO	▸REQ.HAN.HKS2.60 ▸REQ.NFA.AuditEvents.10			Anmeldung mit Nutzername und Passwort erfolgreich	SYS USER
	[1]	name	Benutzername		
FNN.5001.1 WARNING	▸REQ.HAN.HKS2.30 ▸REQ.NFA.AuditEvents.10			Anmeldung mit Nutzername und Passwort fehlgeschlagen	SYS

Log-ID	Anforderung			Zeitpunkt / Ereignis	Logs
	[1]	name	Benutzername		
FNN.5003.0 INFO	▸REQ.NFA.AuditEvents.10			TLS-Proxy-Verbindung zwischen SMGW und CLS erfolgreich aufgebaut	SYS
	[1]	name	Kommunikationsszenario		
	[2]	name	Proxy-ID		
FNN.5003.1 ERROR	▸REQ.HKS.TLSPROXY.CLI.30 ▸REQ.HKS.TLSPROXY.SRV.30 ▸REQ.HKS.TLSPROXY.SOCKS.30 ▸REQ.NFA.AuditEvents.10			TLS-Proxy-Verbindungsaufbau zwischen SMGW und CLS fehlgeschlagen	SYS
	[1]	name	Kommunikationsszenario		
	[2]	name	Proxy-ID		
FNN.5003.2 ERROR	▸REQ.HAN.HKS4.40			TLS-Proxy-Verbindungsaufbau zwischen SMGW und CLS fehlgeschlagen	SYS
	[1]	name	Kommunikationsszenario		
	[2]	name	Gerätespezifischer Fehler		
BSI.20033.0 INFO	▸REQ.FA.DoChangeUserPassword.30 ▸REQ.NFA.AuditEvents.10			Die Letztverbraucher-Zugangsdaten wurden aktualisiert	SYS USER
	[1]	name	userId des geänderten HAN-Kommunikationsprofils		
FNN.5001.2 ERROR	▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.20 ▸REQ.HAN.HKS2.30			Die Anmeldung mit Benutzername/Passwort ist fehlgeschlagen	SYS ALLUSER
BSI.20036.0 INFO	▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.30 ▸REQ.FA.ExportCalLog.90			Teile des Eichlogs wurden ausgelesen	SYS CAL
	[1]	String	SubjectCN des TLS-Zertifikates des authentifizierten Nutzers		
	[2]	String	Query-Filterparameter		
FNN.13006.0 INFO	▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.20 ▸REQ.NFA.AuditEvents.30			Die Systemzeit wurde von Winter- auf Sommerzeit umgestellt	SYS CAL ALLUSER
FNN.13007.0 INFO	▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.20 ▸REQ.NFA.AuditEvents.30			Die Systemzeit wurde von Sommer- auf Winterzeit umgestellt	SYS CAL ALLUSER
BSI.19016.0 INFO	▸REQ.NFA.AuditEvents.10			Start der Syslog-Audit Analyse Funktion	SYS
BSI.19016.1 WARNING	▸REQ.NFA.AuditEvents.10			Stop der Syslog-Audit Analyse Funktion	SYS
BSI.19013.0 INFO	▸REQ.NFA.AuditEvents.10			Start der Syslog-Audit Funktion	SYS
BSI.19013.1 WARNING	▸REQ.NFA.AuditEvents.10			Stop der Syslog-Audit Funktion	SYS
BSI.19017.1 WARNING	▸REQ.NFA.AuditEvents.10			Nicht ausgelesene Syslog-Einträge werden überschrieben	SYS

Log-ID	Anforderung			Zeitpunkt / Ereignis	Logs
BSI.19018.1 WARNING	▸REQ.NFA.AuditEvents.30 ▸REQ.NFA.AuditEvents.10			Nicht ausgelesene Userlog-Einträge werden überschrieben	SYS USER
	[1]	name	UserId		
BSI.19020.1 WARNING	▸REQ.NFA.AuditEvents.30 ▸REQ.NFA.AuditEvents.10			Nicht ausgelesene Eichlog-Einträge werden überschrieben	SYS USER
	[1]	name	UserId		
PTB.19002.1 WARNING	▸REQ.NFA.AuditEvents.10			Eine Überwachungsfunktion hat die Komponente neu gestartet	SYS CAL NOTIFY
	[1]	String	Name der Komponente		
FNN.19003.2 ERROR	▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.30			Der Bootvorgang des Betriebssystems wurde aufgrund eines Fehlers abgebrochen	SYS CAL
	[1]	String	Gerätespezifischer Fehlercode		
FNN.19003.1 WARNING	▸REQ.NFA.AuditEvents.10			Der Bootvorgang des Betriebssystems abgeschlossen. Eine Anomalie ist aufgetreten	SYS
	[1]	String	Gerätespezifischer Fehlercode		
FNN.19004.1 ERROR	▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.30			Der Bootvorgang der SMGW Anwendungssoftware wurde aufgrund eines Fehlers abgebrochen	SYS CAL
	[1]	String	Gerätespezifischer Fehlercode		
	[2]	name	Typ der Datei (z.B. OBIS-ID)		
	[3]	String	Fehlergrund		
BSI.1015.1 WARNING	▸REQ.NFA.AuditEvents.10			Replay einer älteren Nachricht empfangen	SYS
	[1]	hüid	Identifikation der sendenden Messeinrichtung		
BSI.4010.1 WARNING	▸REQ.NFA.AuditEvents.10			Die Sicherheitsfunktionalität ist durch einen temporären Fehler gestört	SYS NOTIFY
	[1]	String	gerätespezifischer Fehlercode		
BSI.4010.2 FATAL	▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.30			Die Sicherheitsfunktionalität ist durch einen dauerhaften Fehler gestört	SYS CAL NOTIFY
	[1]	String	gerätespezifischer Fehlercode		
BSI.7001.7 WARNING	▸REQ.NFA.AuditEvents.10 ▸REQ.WAN.WakeUpSicherung.80			Replay einer älteren Nachricht empfangen	SYS
	[1]	name	Schnittstellenbezeichnung		
BSI.7001.4 ERROR	▸REQ.NFA.AuditEvents.10			Es wurde ein ungültiges Wake-Up-Paket empfangen	SYS
	[1]	name	Schnittstellenbezeichnung		
BSI.19001.1 FATAL	▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.30			Die Integrität des SMGW wurde verletzt oder kann nicht mehr sichergestellt werden	SYS CAL ALLUSER NOTIFY
	[1]	name	Gerätespezifischer Fehlercode		
FNN.19004.2 WARNING	▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.20 ▸REQ.NFA.AuditEvents.30			Der Startvorgang der SMGW-Firmware wurde abgeschlossen. Dabei ist ein Fehler aufgetreten.	SYS CAL ALLUSER
	[1]	name	Gerätespezifischer Fehlercode		

Log-ID	Anforderung			Zeitpunkt / Ereignis	Logs
FNN.19008.2 FATAL	▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.30			Die Kapazität des Eichlogs ist erschöpft.	SYS CAL ALLUSER NOTIFY
BSI.19014.0 INFO	▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.30			Start der Eichlog-Audit Funktion	SYS CAL
BSI.19014.1 WARNING	▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.30			Stop der Eichlog-Audit Funktion	SYS CAL
BSI.19015.0 INFO	▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.20			Start der Userlog-Audit Funktion	SYS ALLUSER
BSI.19015.1 WARNING	▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.20			Stop der Userlog-Audit Funktion	SYS ALLUSER
BSI.13009.0 INFO	▸REQ.NFA.AuditEvents.10 ▸REQ.NFA.AuditEvents.20 ▸REQ.NFA.AuditEvents.30 ▸REQ.FA.UpdateWanComProfile.50			Parameter der Zeitsynchronisation geändert	SYS CAL ALLUSER
	[1]	name	Parametername		
	[2]	String	Parameterwert		
BSI.1018.1 ERROR	▸REQ.NFA.AuditEvents.10			Nachricht konnte nicht authentifiziert werden	SYS
	[1]	hüid	Geräteidentifikation		
BSI.19019.0 INFO	▸REQ.NFA.AuditEvents.10 ▸REQ.FA.DoDeleteUserData.40			Reset (Datenlöschung) des SMGW erfolgreich durchgeführt	SYS CAL
	[1]	String	GWA/SRV-Identifikation		
BSI.19019.1 ERROR	▸REQ.NFA.AuditEvents.10 ▸REQ.FA.DoDeleteUserData.40			Reset (Datenlöschung) des SMGW aufgrund eines Fehlers nicht durchgeführt	SYS
	[1]	String	GWA/SRV-Identifikation		
	[2]	String	Fehlerbeschreibung		
BSI.19022.0 INFO	▸REQ.FA.DoResetTamperState.30			Manipulation zurückgesetzt	SYS CAL USER
	[1]	hüid	Identifikation des manipulierten Gerätes		
BSI.19022.1 ERROR	▸REQ.FA.DoResetTamperState.30			Manipulation konnte nicht zurückgesetzt werden	SYS
	[1]	hüid	Identifikation des manipulierten Gerätes		
BSI.19023.0 INFO	▸REQ.NFA.AuditEvents.10			Anforderung auf ein sicherheitsrelevantes Objekt zuzugreifen	SYS
	[1]	String	Identifikation der beabsichtigten Operation		
	[2]	String	Identifikation des Objekts		
	[3]	String	Identifikation des Subjekts		
BSI.19024.0 INFO	▸REQ.FA.UpdateHanUserProfile.90			Erfolgreiches Ändern der Aufbewahrungsfrist für das Anschlussnutzerlogbuch	SYS CAL USER
	[1]	Number	Anzahl der Tage auf die die Vorhaltefrist geändert wurde		
	[2]	Number	Einträge gelöscht		
BSI.19024.1 ERROR	▸REQ.FA.UpdateHanUserProfile.90			Aufbewahrungsfrist für das Anschlussnutzerlogbuch konnte nicht geändert werden	SYS CAL USER

Log-ID	Anforderung		Zeitpunkt / Ereignis	Logs
	[1]	Number	Anzahl der Tage auf die die Vorhaltefrist geändert werden sollte	

Tabelle A.1 Liste aller zu protokollierenden Ereignisse

Anhang B Abkürzungsverzeichnis

Abkürzung	Beschreibung
aEMT	Aktiver Externer Marktteilnehmer
AFL	Authentication and Fragmentation Layer, Wireless MBUS
API	Application Programming Interface
APL	Application Protocol Layer, Wireless MBUS
APN	Access Point Name (Zugangspunkt zum WAN)
ARP	Address Resolution Protocol
ASN	Abstract Syntax Notation
AWL	Abgeleitete Werteliste
BER	Basic Encoding Rules (ASN.1)
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CLS	Controllable Local System
CMS	Cryptographic Message Syntax, Inhaltsdatensicherung nach ASN.1
CON	Consumer bzw. Anschlussnutzer
COSEM	COmpanion Specification for Energy Metering
DER	Distinguished Encoding Rules (ASN.1)
DS	Detailspezifikation
EMS	Energie-Managmenet-System
EMT	Externer Marktteilnehmer
EnWG	Energiewirtschaftsgesetz
FA	Fachlicher Anwendungsfall
FAKAT	Kategorie fachlicher Anwendungsfälle
GDEW	Gesetz zur Digitalisierung der Energiewende
GWA	Smart-Meter-Gateway-Administrator
GWH	Smart-Meter-Gateway-Hersteller
HAN	Home Area Network
HDLC	High Level Data Link Control
HKS	HAN-Kommunikationsszenario
HTTP	HyperText Transfer Protocol
IC	Interface Class (für COSEM)
ICS	Implementation Conformance Statement
IETF	Internet Engineering Task Force
IP	Internet Protocol
KS	Kommunikationsszenario
LKS	LMN-Kommunikationsszenario
LMN	Local Meter Network
wM-Bus	Wireless Meter Bus
MAC	Medium Access Control
MessEG	Mess- und Eichgesetz

Abkürzung	Beschreibung
MessEV	Mess- und Eichverordnung
MK	Master Key
MSB	Messstellenbetreiber
MsbG	Messstellenbetriebsgesetz
MTR	Messeinrichtung
N/A	Nicht anwendbar
NDS	Netzwerk Diagnose Service
NTP	Network Time Protocol
NWL	Nicht-validierte Werteliste
OBIS	OBject Identification System (für COSEM)
OUI	Organizational Unique Identifier (Herstellerspezifischer Adress-Prefix)
PSK	Pre-Shared Key, zuvor vereinbarter symmetrischer Schlüssel
PTB	Physikalisch-Technische Bundesanstalt
RFC	Request For Comments
RTT	Round Trip Time
RWL	Registrierte Werteliste
SM	Sicherheitsmodul
SM-PKI	Smart-Meter - Public Key Infrastructure
SMGW	Smart-Meter-Gateway
SML	Smart Message Language
SNI	Server Name Indication
SRV	Servicetechniker des SMGW
TCP	Transmission Control Procotol
TLS	Transport Layer Security, Transportsicherungsprotokoll
TPL	Transport Protocol Layer, Wireless MBUS
TR	Technische Richtlinie
TWL	Tageswerte Liste
UDP	User Datagram Protocol
UTC	Coordinated Universal Time, Zeitskala
WAN	Wide Area Network
WKS	WAN-Kommunikationsszenario
XML	Extendable Markup Language

Tabelle B.1 In der TR verwendete Abkürzungen

Anhang C Lokale Zugriffsrechte

Dieser Anhang enthält eine Übersicht über die Berechtigungsprüfung lokaler Nutzer zum Zugriff auf Ressourcen und Dienste des SMGW. Die Berechtigungsprüfung basiert auf der nachgewiesenen Rolle und Identität des Nutzers und dem Zugriff über eine lokale Schnittstelle. Die Rollen basieren auf den lokalen Rollen SRV, CON, CLS des [PP-0073] und werden durch diesen Anhang künftig weiter differenziert. Die Tests zur TR-03109-1 prüfen, dass ein Zugriff gemäß Tabelle möglich ist (Mindestanforderung), die IT-Sicherheitstests gemäß [PP-0073] weisen nach, dass ein unberechtigter Zugriff nicht möglich ist.

Das Regelwerk (Policy) zur attribut-basierten Berechtigungsprüfung setzt sich aus einem statischen Teil (definiert über HAN-Kommunikationsszenarien) und einem dynamischen Teil (definiert über die vom GWA konfigurierten HAN- und Proxy-Kommunikationsprofile) zusammen.

Die Terminologie der Autorisierungspolicies (PEP, PDP etc.) ist aus RFC2904 (AAA Authorization Framework) bzw. Oasis XACML übernommen, aber hier auf das Wesentliche reduziert. (RBAC=Role Based Access Control, ABAC = Attribut Based Access Control).

Zugriff auf TLS-Proxy Dienste wird nur der Rolle "CLS" gewährt.

▸Abbildung C.1 zeigt den Ablauf der Berechtigungsprüfung zum Zugriff auf Ressourcen des SMGW.

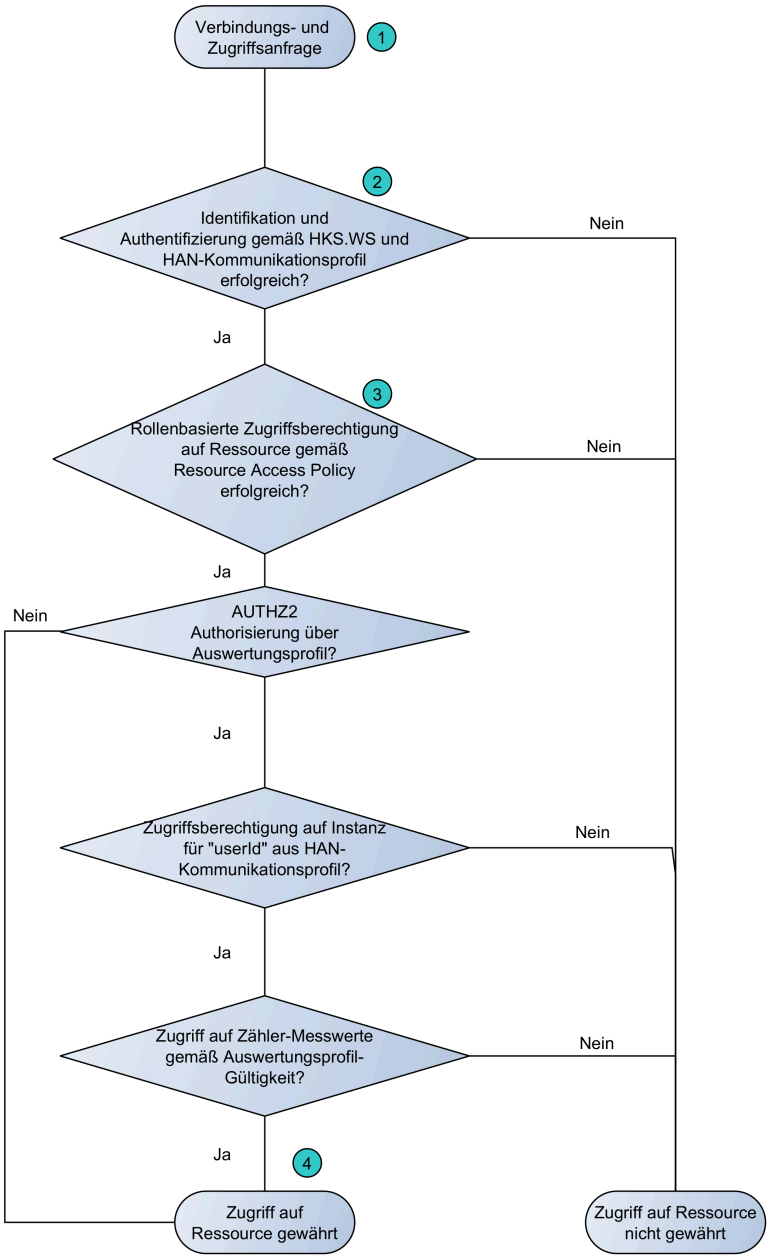


Abbildung C.1. Ablauf der Berechtigungsprüfung beim lokalen Zugriff auf Ressourcen des SMGW

▸Abbildung C.2 zeigt die funktionale Sicht auf die Berechtigungsprüfung beim lokalen Zugriff auf Ressourcen des SMGW.

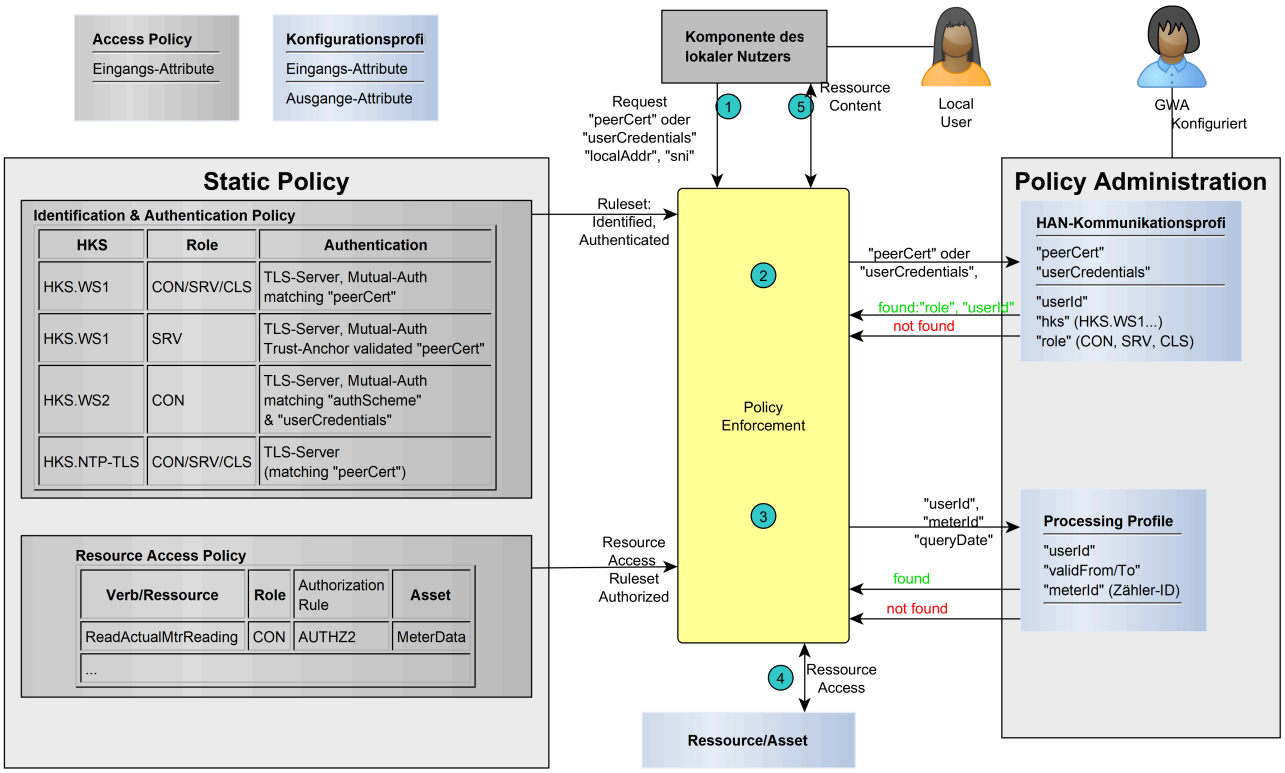


Abbildung C.2. Übersicht über die Attribut-basierte Berechtigungskontrolle beim lokalen Zugriff auf Ressourcen des SMGW

Zugriff auf Ressource (FA/Dienst)	Rolle	Autorisierungsbedingungen	Asset
▸FA.ReadInstantMtrReading, ▸FA.ReadTariffState	CON, CLS	AUTHZ2	Meter data
▸FA.ExportDailyMtrReading, ▸FA.ExportRegMtrReading, ▸FA.ExportDerivedMtrReading	CON	AUTHZ2	Meter data
▸FA.ReadTimeSyncStatus	CON, SRV, CLS	AUTHZ1	SMGW time
▸FA.ReadProxyChStatus	CLS	AUTHZ5	Communication profile
▸FA.DoRequestProxyCh	CLS	AUTHZ6	Communication profile
▸FA.DoCloseProxyCh	CLS	AUTHZ6	-
▸FA.NtpTimeService	SRV, CON, CLS	AUTHZ7	SMGW time
▸FA.DoCreateKeyPairAndClsCert	CLS	AUTHZ1	HAN device key pair
▸FA.ExportUserLog	CON	AUTHZ4	Consumer log data (für "userId")
▸FA.ReadProcessingProfile	CON, CLS	AUTHZ4	Processing profile
▸FA.ListSmgwResources	CON, SRV, CLS	AUTZH3	-
▸FA.ExportSysLog	SRV	AUTHZ1	System log data
▸FA.ExportCalLog, ▸FA.DoTruncateCalLog	SRV	AUTHZ1	Calibration log data
▸FA.ReadNetworkIfStatus	SRV	AUTHZ1	-
▸FA.ReadWanIfProfile	SRV	AUTHZ1	-
▸FA.UpdateWanIfProfile	SRV	AUTHZ1	-
▸FA.ReadHanIfProfile	SRV	AUTHZ1	-
▸FA.ReadLmnIfProfile	SRV	AUTHZ1	-

Zugriff auf Ressource (FA/Dienst)	Rolle	Autorisierungsbedingungen	Asset
▸FA.DoSelftest	SRV	AUTHZ1	-
▸FA.UpdateWanComProfile	SRV	AUTHZ1	Communication profile
▸FA.ReadLmnComProfile	SRV	AUTHZ1	Communication profile, Certificates
▸FA.ReadWanComProfile	SRV	AUTHZ1	Communication profile, Certificates
▸FA.ReadHanComProfile	SRV	AUTHZ1	Communication profile, Certificates
▸FA.ReadProxyComProfile	SRV	AUTHZ1	Communication profile, Certificates
▸FA.ReadCertificate	CON, SRV, CLS	AUTHZ1	Certificates
▸FA.ListIdentifiedMeters	SRV	AUTHZ1	Communication profile
▸FA.ListIdentifiedCls	SRV	AUTHZ1	Communication profile
▸FA.ReadDeviceInfo	CON, SRV, CLS	AUTHZ1	Communication profile
▸FA.ReadDeviceStatus	CON, SRV	AUTHZ1	Communication profile
▸FA.DoReboot	SRV	AUTHZ1	-
▸FA.DoDeleteUserData	SRV	AUTHZ1	Personal identifiable information
▸FA.ReadStartPage	CON	AUTHZ1	-
▸FA.DoLogout	CON, CLS, SRV	AUTHZ1	-
▸FA.DoChangeUserPassword	CON	AUTHZ1	Consumer password hash
▸FA.DoRemoveSmgwAssocInMtr	SRV	AUTHZ1	-

Tabelle C.1 Resource Access Policy (Zugriffsrechte lokaler Nutzer auf Ressourcen des SMGW)

Durch den GWA dynamisch für die Zugriffskontrolle konfigurierte Zugriffs-Attribute sind:

- Rolle (CON, CLS, SRV) aus dem HAN-/Proxy-Kommunikationsprofil, dass zur Authentifizierung verwendet wurde,
- "userId" (aus HAN-Kommunikationsprofil für CON),
- Ressource/Dienst-Identifikation.

Durch die TR-03109-1 statisch für die Zugriffskontrolle vorgegebene Zugriffs-Attribute sind:

- Zugriff nur über die HAN-Schnittstelle,
- HKS (vorgegebene IT-Sicherheitsprotokolle, TLS-Rolle Client/Server, Applikationsdienstrolle Client/Server, kryptografische Verfahren).

Bezeichner der Regel	I&A	Autorisierungsbedingungen
AUTHZ1	Lokaler Nutzer authentifiziert und identifiziert mit HAN-Kommunikationsprofil HKS.WS1 ("peerCert") oder HKS.WS2 ("userCredentials").	Zugriffsverb übereinstimmend mit FA-Verb (Read, Create, Update, Delete, Do) gemäß ▸Tabelle C.1
AUTHZ2		• Zugriffsverb übereinstimmend mit FA-Verb (Read, Create, Update, Delete, Do) gemäß ▸Tabelle C.1. • Der "userId" aus dem HAN-Kommunikationsprofil ist ein Auswertungsprofil zugeordnet. • Zugriff auf Messdaten für die im Auswertungsprofil referenzierte "meterId". • Historische Daten sind darüber zeitlich begrenzt auf den Gültigkeitszeitraum des Auswertungsprofiles.
AUTHZ3		Lesender Zugriff auf Metadaten der Ressourcen gemäß ▸Tabelle C.1.

Bezeichner der Regel	I&A	Autorisierungsbedingungen
AUTHZ4		• Zugriff übereinstimmend mit FA-Verb (Read, Create, Update, Delete, Do) gemäß ▸Tabelle C.1. • Der "userId" aus dem HAN-Kommunikationsprofil ist die Ressource gemäß FA zugeordnet (z.B. UserLog).
AUTHZ5		• Übereinstimmung des "localPeerCert" des Proxy-Kommunikationsprofils mit dem "peerCert" des HAN-Kommunikationsprofiles. • Zugriff auf Betriebszustand des TLS-Proxy-Kanals übereinstimmend mit FA-Verb (Read, Create, Update, Delete, Do) gemäß ▸Tabelle C.1.
AUTHZ6	Lokaler Nutzer authentifiziert und identifiziert mit Proxy-Kommunikationsprofil ▸HKS.TLSPROXY.CLI, ▸HKS.TLSPROXY.SRV, ▸HKS.TLSPROXY.SOCKS ("localPeerCert")	Änderung des Betriebszustandes des TLS-Proxy-Kanals, der über die Signalisierung im Verbindungsaufbau übereinstimmend mit dem Proxy-Kommunikationsprofil Parametern "localServerName"/"wanPeerAddress" identifiziert wird.
AUTHZ7	SMGW authentifiziert sich über ▸HKS.NTP-TLS.SRV	Keine Authentifizierung der Rolle erforderlich.

Tabelle C.2 Bedingungen für attributbasierte Autorisierung des Zugriffs

Anhang D Anwenderhinweise für den MSB

Dieser Anhang enthält Hinweise zur bestimmungsgemäßen Verwendung des SMGW im Intelligenten Messsystem (iMSys). Verwender des SMGW ist im Sinne des [MsbG] der Messstellenbetreiber (MSB), als Betreiber des SMGW.

Weitere nicht-normative Hinweise zum vorgesehen Betrieb des SMGW sind in [TR-03109-1-VI] beschrieben.

Nummer	Hinweis
Kommunikative Anbindung im LMN	
LMN1	Ein an das SMGW angebundener Kommunikationsadapter darf nur genau einer Messeinrichtung zugeordnet sein, da die Identifikation und Nichtabstreitbarkeit der Herkunft der Messwerte eindeutig mit der kryptografischen Identität des Kommunikationsadapters (TLS-Zertifikat) verknüpft ist.
LMN2	Ein kommunikativ an das SMGW angebundener Kommunikationsadapter einer Messeinrichtung darf nicht physisch von der ihr zugeordneten Messeinrichtung getrennt werden, um sie mit einer anderen Messeinrichtung zu verwenden. Das gilt für Messeinrichtungen und Kommunikationsadapter aller Sparten.
LMN3	Da die Zeitstempelung von Messwerten zum Empfangszeitpunkt im SMGW stattfindet, muss die maximale nicht-vernachlässigbaren Kommunikationslatenz gemäß ▸ICS.FA.CaptureRequestedMtrData.10 und ▸ICS.FA.CaptureUnsolicitedRcvdMtrData.10 (Max. 4 Sekunden) zwischen Messwertbildung und Erfassung im SMGW durch die gewählte Kommunikationstechnologie zwischen Messeinrichtung und SMGW mindestens zu 99 % der Messwertübertragungen eingehalten werden können. Zu berücksichtigen sind dabei: • bei Kommunikationstechnologien in gemeinsam genutzten Medien (z.B. RS-485 Bus, Funk- oder Powerline-Technologien) die Anzahl der Kommunikationsteilnehmer im Kanal, • die maximale zulässige relative Einschaltdauer (Duty Cycle) für das Funkband zwischen Messeinrichtung und SMGW, • die Medien-Zugangsbeschränkung (Media Access Control) zur Kollisionsvermeidung zwischen den Kommunikationsteilnehmern, • die Möglichkeit beabsichtigter Störungen des Mediums ("Jamming"), • Störungen des Mediums durch schlechtes Signal-Rausch-Verhältnis z.B. durch Dämpfung auf dem Weg zwischen Messeinrichtung und SMGW, • eine ausreichende Datenrate bzw. Bandbreite für die Nutzung des TLS-Protokolls für die notwendige Zahl von Kommunikationspartnern. Sofern diese Auflage nicht zu jedem Zeitpunkt eingehalten werden kann, muss die Messeinrichtung in der Anwendungsnachricht eine Information enthalten, aus der das SMGW die Aktualität bzw. Laufzeit berücksichtigen kann. Für eine mittels ▸LKS1 angebundene Messeinrichtung siehe dazu [DS] Kapitel "SML" Abschnitt "Zeitliche Anforderungen". Für eine mittels ▸LKS2 angebundene Messeinrichtung siehe dazu [DS] Kapitel "Wireless M-Bus Protokoll" Abschnitt "Zeitliche Anforderungen".
LMN4	Kommunikationsadapter und Messeinrichtung müssen über eine physisch gesicherte (z.B. gemeinsames Gehäuse) oder IT-gesicherte Kommunikation miteinander verbunden sein, die den Anforderungen gemäß [TR-03109-3] genügt.
LMN5	Sofern ein gemeinsam genutztes Kommunikationsmedium[1] zwischen Messeinrichtung und SMGW verwendet wird, muss jederzeit durch gewährleistet sein, dass die Anwendungsfälle des SMGW (insbesondere Messwertauslesung 15Minuten, Netzzustandsdaten minütlich) für jede im SMGW konfigurierte Messeinrichtung umgesetzt werden können. Dabei sind die einschlägigen Normen für das physische Medium zu berücksichtigen. Für ▸LKS1 (RS-485) ist die Guard-Time, HDLC-Telegrammlänge, Transceiver-Umschaltzeit gemäß [VDE0418-63-7] zu berücksichtigen. Für ▸LKS2 (wM-Bus) ist die relative Einschaltdauer ("Duty Cycle") gemäß [EN13757-4] aller unaufgeforderten Sender zu berücksichtigen.

[1] z.B. Bus, Funkband, drahtgebundene Modulationstechniken

Nummer	Hinweis
LMN6	Messeinrichtungen für Elektrische Energie mit Niederspannungsanschluss, die zur Abrechnung, zur energiewirtschaftlichen Bilanzierung oder zur Umsetzung weiterer gemäß [MsbG], [EnWG] oder [EEG] regulierter Anwendungsfälle verwendet werden, sind über die LMN-Kommunikationsschnittstelle an das SMGW kommunikativ anzubinden.
GWA/MSB Aufgaben	
GWA1	entfallen
GWA2	Die Eineindeutigkeit der vom MSB oder GWA gewählten "tafId" der Auswertungsprofile muss über alle SMGW gewährleistet sein.
GWA3	Stellt der GWA des MSB eine Abweichung des SMGW-Zeitstempels um mehr als +/-3 % der Registrierperiodendauer von der gesetzlichen Zeit fest, informiert er den MSB über diesen Vorfall. Der MSB informiert den Messwertverwender über diesen Vorfall.
GWA4	Der GWA gewährleistet die referentielle Integrität der Konfigurationsprofile solange die Profile für die Datenverarbeitung verwendet werden. Dazu gehört die Gewährleistung der Eindeutigkeit der im SMGW konfigurierten Profil-IDs und der Verweise auf andere Profile.
GWA5	Der GWA muss in Zusammenarbeit mit dem MSB der zuständigen Stelle nach § 40 MessEG und § 48 MessEG auf Anforderung den Inhalt des Eichlogs auf Anforderung zur Verfügung stellen. Er muss die geforderten Informationen unverzüglich, unverändert und vertraulich an die zuständige Stelle weiterleiten. Hierbei ist zu beachten, dass dies auch bei Verwendung von ▸FA.DoDeleteUserData und ▸FA.DoTruncateCalLog sichergestellt werden muss.
GWA6	Die Einrichtung einer Zugriffsberechtigung des CLS auf Messwerte (Konfiguration einer CLS-ID im Auswertungsprofil) setzt einen berechtigten Zweck oder die Einwilligung des Endkunden voraus.
GWA7	Der GWA gewährleistet bei der Konfiguration eines WAN-Kommunikationsprofiles vom Typ "WKS.TLSPROXY", dass der EMT die Voraussetzungen an einen aktiver EMT gemäß SM-PKI-CP erfüllt.
GWA8	Der GWA gewährleistet die Validität der Datenfelder der zu importierenden Konfigurationsprofile, sofern dies nicht vom SMGW gewährleistet wird. Siehe SOLL-Anforderungen und ICS zur Validierung in den **FA.Create...Profile** und **FA.Update...Profile**.
Kommunikative Anbindung im WAN	
WAN1	Zur Gewährleistung einer leistungsfähigen Fernkommunikation (§ 21 Abs 1 Nr. 3 MsbG) berücksichtigt der MSB bei der Auswahl der Fernkommunikationstechnik: • bei Kommunikationstechnologien in gemeinsam genutzten Medien (z.B. Bus, Funk- oder Powerline-Technologien) die Anzahl der Kommunikationsteilnehmer im Kanal, • die Möglichkeit beabsichtigter Störungen des Mediums ("Jamming"), • Störungen des Mediums durch schlechtes Signal-Rausch-Verhältnis z.B. durch Dämpfung auf dem Weg vom Zugangspunkt zur Messstelle, • eine ausreichende Datenrate bzw. Bandbreite für die Nutzung des TLS-Protokolls für die notwendige Zahl von Kommunikationsverbindungen. • ein Firmware-Update des SMGW innerhalb eines Zeitraumes durchgeführt werden kann, der die Aufgaben des GWA gemäß [TR-03109-6] und des MSB gewährleistet.
WAN2	Alle EMT- und GWA-Kommunikationssysteme unterstützen die in [DS] Kapitel "CMS" definierten Formate, Algorithmen und Parameter für die WAN-Kommunikation mit dem SMGW.
Messwertverwendung	
MWV1	Zentrale Tarifierung: Wird eine Tarifstufenzuordnung - auf Basis von TAF7 Zählerstandsgängen - nicht im SMGW vorgenommen, dann dürfen die Regelwerkparameter (z.B. Tarifstufenzuordnungen) nicht während des Abrechnungszeitraumes geändert werden und müssen dem Rechnungsempfänger bekannt gemacht werden (z.B. über eine Online-Schnittstelle).
MWV2	Der Verwender muss die vom SMGW bereitgestellten Messwertstatusinformationen insbesondere zur Validität und Qualität der Messwerte und zur Integrität der Messeinrichtung und des SMGW bei der Verarbeitung berücksichtigen. Siehe dazu [VDE4400] sowie [DVGW-G685-4] und [DVGW-G685-5].

Nummer	Hinweis
MWV3	Der GWA gewährleistet dass bei Konfiguration mehrerer abrechnungsrelevanter Auswertungsprofile zu einer Messeinrichtung zu einem Registrierzeitpunkt keine widersprüchlichen (z.B. voneinander abweichenden) Messwerte im SMGW registriert werden ("Unzulässige Mehrfachtarifierung"). Für eine Messeinrichtung dürfen keine Auswertungsprofile mit überlappendem Gültigkeitszeitraum konfiguriert sein, die sowohl in der Messeinrichtung registrierte, als auch im SMGW registrierte Messwerte an den EMT bereitstellen.
MWV4	Der MSB/GWA gewährleistet bei der Konfiguration des TAF8, dass die Auflösung und Anzahl signifikanter Stellen der von der Messeinrichtung gelieferten Zählerstände zur Einhaltung der Fehlergrenzen der berechneten Leistung gemäß MessEV für die konfigurierte Registrierperiode geeignet ist.

Tabelle D.1 Hinweise zur Verwendung

Anhang E Changelog

Nr.	Fundstelle überarbeitete Version	Änderung im Vergleich zur Vorversion
Struktur 1	Allgemein	Globale Anpassung der Struktur der technischen Richtlinie durch Umbau auf fachliche Anwendungsfälle (Details enthalten die nachfolgenden Zeilen).
Struktur 2	▸Kapitel 3	Anforderungen der Anwendungsfälle (WAF, HAF, LAF) wurden aus dem Kapitel "Anforderungen an die Kommunikationsverbindungen und Protokolle des SMGW" in das neue ▸Kapitel 3 überführt, um eine klarere Trennung zwischen Anforderungen an die Kommunikation und die Funktionalität zu erreichen. Diese Anforderungen wurden dabei durch weitere Anforderungen detailliert und Bilden die Basis erstellter fachlicher Anwendungsfälle (FA). Anforderungen und Funktionen, die auf diese Weise mit weiteren Details und Anforderungen hinterlegt wurden, werden in diesem Changelog im Gegensatz zu neuen Funktionen nicht weiter detailliert.
Struktur 3	▸Kapitel 3	Anforderungen aus den ehemaligen Kapiteln 3, 4 und 5 wurden auf Basis ihres Zwecks in passende fachliche Anwendungsfälle und FA-Kategorien eingeordnet bzw. aufgelöst.
Struktur 4	▸Kapitel 3, ▸Kapitel 4	Reihenfolge umgekehrt: Anforderung in Form fachlicher Anwendungsfälle kommen nun vor den Anforderungen an die Kommunikationsszenarien.
Struktur 5	▸FAKAT.NetworkDiagnosis	Die Beschreibung des Netzwerkdiagnoseservice wurde aus der Detailspezifikation in die TR-03109-1 überführt und in die FA-Struktur umgebaut. Sie ist inhaltlich jedoch unverändert.
Struktur 6	▸Kapitel 4	Anforderungen an Kommunikationsszenarien wurden teilweise in die Detailspezifikation überführt und durch Verweise ersetzt.
Struktur 7	▸Anhang D	Verwenderauflagen, die aus der Integration der PTB A50.8 entstanden sind wurden in die TR-03109-1 überführt.
Daten1	▸Abschnitt 3.22	Neu: Datenstrukturen werden auf semantischer (und abstrakt syntaktischer) Ebene definiert. Dies stellt eine Konkretisierung der Profildefinitionen der vorherigen Version dar. Des Weiteren wurden neue Datenstrukturen zur Erfüllung neuer Funktionalität definiert. Die definierten Datenstrukturen dienen als Basis zur Ableitung der im Rechtsrahmen geforderten Anwendungsprogrammierschnittstellen und Prozessbeschreibungen. Des Weiteren ist die Definition von Datenstrukturen für die Integration von Anforderungen aus der PTB-A 50.8 notwendig. Zur Verbesserung der Migrationsfähigkeit der Datenstrukturen und um Kompatibilität mit herstellerspezifische Varianten der vorherigen Version zu vereinfachen, sind einige Datenfelder optional. Sofern die Datenfelder nicht vorhanden sind, verwendet das SMGW stattdessen Standardwerte.

Nr.	Fundstelle überarbeitete Version	Änderung im Vergleich zur Vorversion
Daten2	▸Abschnitt 3.22	Neu: für Messwertlisten wurden neue Datenstrukturen eingeführt: • Registrierte Werteliste (RWL): dient der Speicherung registrierter Werte, die versandt oder zur Ableitung neuer Messgrößen verwendet werden. In der PTB-A 50.8 als "originäre Messwertliste" bezeichnet. Die Umbenennung erfolgte auch, weil die originären Werte in registrierenden Messeinrichtungen nicht im SMGW sondern in der Messeinrichtung gebildet werden. • Abgeleitete Werteliste (AWL): dient der Speicherung abgeleiteter Werte bzw. abgeleiteter Register, die aus registrierten Werten bestimmt wurden. In der PTB-A 50.8 ebenfalls als "abgeleitete Messwertliste" bezeichnet. • Tageswerteliste (TWL): dient der Speicherung von Tageswerten. RWL und AWL wurden zur Integration von Anforderungen aus der PTB-A 50.8 eingeführt. Die TWL wurde zur Erfüllung des Rechtsrahmens (§ 61 und 62 MsbG) bei gleichzeitiger Einsparung von Speicherplatz im SMGW über den Vorhaltezeitraum eingeführt. Da an die Tageswerte nicht die höheren Anforderungen an zeitliche Fehlergrenzen zur gesetzlichen Zeit gestellt werden, aber längere Vorhaltefristen gelten, wird dem Implementierer die Möglichkeit gegeben beim Export TWL aus Registrierten Wertelisten zu erzeugen oder separate Ringspeicher vorzusehen.
Daten3	▸Abschnitt 3.22	Neu: für den Export verschiedener Daten (Logs, Wertelisten) wurden eine einheitliche Datenstruktur definiert (genannt Exportstruktur). Diese findet sowohl an WAN (Messwertversand) als auch an HAN (Bereitstellung für Anschlussnutzer) Verwendung. Die konkrete Transfersyntax unterscheidet sich jedoch an den verschiedenen Schnittstellen. Der Export erlaubt die Bereitstellung von signierten Messwerten, wobei eine Signatur des SMGW über alle Messwerte gebildet wird, statt jeden Messwert einzeln zu signieren, was Rechenzeit, Speicher und Datenvolumen einspart. Die Datenstruktur ist besonders im Hinblick auf die Integration der PTB-A 50.8 relevant.
MWV1	▸FAKAT.ValProcBilling ▸FAKAT.ValProcNonBilling ▸FAKAT.ValTransmission ▸FAKAT.ValCapture ▸FAKAT.ConServices	Geändert: die bisher in Kapitel 4 (Messwertverarbeitung für Tarifierung, Bilanzierung und Netzzustandsdatenerhebung) gesammelten Anforderungen wurden in geeignete FA-Kategorien einsortiert: • ▸FAKAT.ValProcBilling: enthält die Beschreibung der zur Abrechnung verwendeten Tarifanwendungsfälle (enthält bisherige TAF1, TAF2 und TAF7). • ▸FAKAT.ValProcNonBilling: enthält die Beschreibung von nicht zur Abrechnung verwendeter Tarifanwendungsfälle (enthält bisherige TAF9, TAF10, TAF14). • ▸FAKAT.ValTransmission: enthält die Funktionalität des Messwertversands zum EMT. • ▸FAKAT.ValCapture: enthält die Funktionalität des Messwertempfangs von der Messeinrichtung. • ▸FAKAT.ConServices: enthält die Dienste für den Anschlussnutzer, zu denen auch die Bereitstellung von Messwerten zählt. Durch die Aufteilung wird die Redundanz von Anforderungen verringert und eine besser Abgrenzung zwischen eichrechtlich relevanten und sonstigen Teilen der Messwertverarbeitung geschaffen.
MWV2	▸Kapitel 3	Neu: die in der PTB-A 50.8 definierten Anforderungen wurden soweit möglich über Anforderungen in der TR abgebildet mit dem Ziel der Vereinfachung und Beschleunigung der Zertifizierungsverfahren. Details sind den weiteren Einträgen dieser Tabelle zu entnehmen.
MWV3	▸FAKAT.ValProcBilling	Neu: Konkretisierungen zum Thema des Messwertempfangs und der Prüfung von Messwerten im Rahmen der Messwertregistrierung auf Basis der PTB-A 50.8.

Nr.	Fundstelle überarbeitete Version	Änderung im Vergleich zur Vorversion
MWV4		Geändert: der bisherige TAF1 ermöglicht nun die Verwendung für weitere Medien.
MWV5	-	-
MWV6	▸FAKAT.ValProcBilling	Geändert: TAF2 wurde um eine einheitliche, einfache Art der Konfiguration ergänzt, die auf den in im Universalbestellprozess der Marktkommunikation verwendeten Zählzeitdefinitionen zur Festlegung des jeweils aktiven Registers basiert. Damit werden Clearing-Probleme des MSB durch kalendarische Tarifstufen-Konfigurationen vermieden. Die Möglichkeit zur Parametrierung über Zeitplänen bleibt zunächst erhalten. Als zusätzliche Funktion erlaubt die Parametrierung des TAF2 für die Tarifstufen Preisbestandteile angeben zu können. In Zukunft können diese Preisbestandteile (sofern vom GWA angegeben) z.B. an EMS weitergegeben werden. Dies kann die Notwendigkeit einer Anbindung von EMS an eine Internet-basierte API zum Einholen solcher Preisbestandteile ersetzen.
MWV7	▸FAKAT.ValProcBilling	Neu: ein neuer TAF zur Bildung von Lastgängen und zur Bestimmung von Maximalwerten (TAF8) wurde eingeführt. Dieser ermöglicht dem MSB eine wirtschaftliche registrierende Lastgangmessung im SMGW zur Messwerterhebung gemäß § 55 MsbG mit einem nicht registrierenden Haushaltszähler.
MWV8	▸FAKAT.ValProcBilling ▸FAKAT.ValCapture	Neu: ein neuer TAF für den Abruf von Messwerten aus registrierenden Messeinrichtungen (TAF15) wurde eingeführt. Dies dient der Anbindbarkeit von registrierenden Messeinrichtungen an das SMGW, wenn dies gemäß MsbG erforderlich ist. Die Registrierung der Messwerte, inkl. Validierung zeitlicher Fehlergrenzen findet dann nicht im SMGW statt.
MWV9	▸FAKAT.ValProcBilling ▸FAKAT.ValProcConfig	Geändert: der TAF6 wurde durch einen FA ersetzt, der das rückwirkende Abrufen von Werten in einem definierten Zeitrahmen ermöglicht.
MWV10	▸FAKAT.ValTransmission	Neu: Möglichkeit für den erneuten Versand von Wertelisten durch den GWA. Die Funktion dient dem nachholenden Versand beim EMT im Fall fehlender Daten. Das SMGW stellt grundsätzlich im Rahmen des Messwertversands sicher, dass alle bisher nicht versandten Messwerte an den EMT übermittelt werden.
MWV11	▸Abschnitt 2.5.2	Neu: Definition der verwendbaren OBIS-Kennzahlen (eingehend und ausgehend). Dies wurde bisher auf Ebene des TAF definiert und war auf die Begrenzung der verwendbaren (eingehenden) Messgrößen beschränkt. Die für die Ableitung und den Messwertversand einsetzbaren OBIS-Kennzahl waren nicht definiert. Mit der Definition wird diese Lücke geschlossen, was im Hinblick auf die Integration der PTB-A 50.8 und den Datenstrukturen/Profilen notwendig ist.
MWV12	▸FAKAT.SmgwTimeSync	Neu: die Anforderungen an die Zeitsynchronisation wurden auf Basis der PTB-A 50.8 konkretisiert und erweitert. Vorgesehen ist die Synchronisation periodisch, auf Veranlassung des GWA und nach einem Neustart. Durch die beschrieben Anforderungen kann die nach PTB-A 50.8 geforderte Synchronisation vor jedem Versand entfallen.
MWV13	▸FAKAT.ValProcBilling ▸FAKAT.ValProcNonBilling	Implementierung optionaler TAF ermöglicht, sofern der TAF in einem BSI Begleitdokument zur TR beschrieben ist.
MGMT1	▸Kapitel 3	Neu: für verschiedene bereits definierte Profile wurde bisher keine Möglichkeit in der TR spezifiziert, diese wieder auslesen zu können. Diese Lücke wurde nun geschlossen und bildet damit die gängige Praxis ab, die diese Funktion bereits umsetzt.
MGMT2	▸FAKAT.EmtComConfig	Neu: Funktionalität für den GWA zur Prüfung der korrekten kommunikativen Anbindung eines EMT. Sinnvoll für Fehlerdiagnose und Betriebsführung.

Nr.	Fundstelle überarbeitete Version	Änderung im Vergleich zur Vorversion
MGMT3	▸FAKAT.EmtComConfig	Neu: Funktionalität zur Aktualisierung von WAN-Kommunikationsprofilen von EMT ergänzt. Das Einspielen und Löschen war bereits gefordert. Für die Aktualisierung bestand bisher keine Vorgabe. Diese Lücke wurde nun geschlossen und bildet nun die gängige Praxis ab, die diese Funktion bereits umsetzt.
MGMT4	▸FAKAT.ValProcConfig	Neu: Funktionalität zum automatisierten Löschen eines Auswertungsprofils und damit verbundener Wertelisten nach Ablauf der Vorhaltefristen ergänzt.
MGMT5	▸FAKAT.SmgwMonitoring	Neu: Möglichkeit zur Verkürzung des Eichlogs auf Veranlassung des GWA ergänzt. Der MSB ist verantwortlich für die Aufbewahrung des Eichlogs über den geforderten Zeitraum. Durch die Möglichkeit der Verkürzung des Eichlogs kann Speicherplatz freigegeben werden. Im Hinblick auf die Nachhaltigkeit und den Entfall einer Eichfrist können SMGW somit langfristig verwendet werden.
MGMT6	▸FAKAT.SmgwMonitoring	Neu: Möglichkeit zur Auflistung der eingespielten Profile und Ressourcen für den GWA ergänzt. Dies ist im Hinblick auf die Betriebsführung und Fehleranalyse sinnvoll. Des Weiteren ist diese Funktion bereits gängige Praxis.
MGMT7	▸FAKAT.SmgwMonitoring	Neu: Möglichkeit zum Auslesen von Informationen über das SMGW und angebundene Komponenten. Die Möglichkeit Informationen über das SMGW auszulesen ist bereits herstellerspezifisch gegeben und wird mit den Anforderungen vereinheitlicht.
MGMT8	▸FAKAT.SmgwMonitoring ▸Anhang A	Neu: die Protokollierung von Ereignissen wird nun interoperabel vorgegeben (siehe andere Punkte dieser Tabelle). In ▸Anhang A wird dabei festgelegt, welche Ereignisse eine direkte Benachrichtigung des GWA über das Kommunikationsszenario ADMIN-SERVICE erfordern. Die Festlegung in ▸Anhang A stellt die Standardkonfiguration für die Benachrichtigung dar. Die Standardkonfiguration kann durch den GWA abgeändert werden, sodass eine Benachrichtigung für bestimmte Ereignisse deaktiviert oder ergänzt werden kann. Die Protokollierung in die relevanten Logs ist davon nicht beeinflusst. Diese Funktionalität erlaubt dem GWA die Anpassung der Benachrichtigung zur Harmonisierung mit den eigenen Prozessen.
MGMT9	▸FAKAT.SmgwAdministration	Neu: Funktionalität zur Aktualisierung der GWA WAN-Kommunikationsprofile ergänzt. Dies erlaubt beispielsweise das Aktualisieren von Adressen, ohne einen komplizierten Wechselprozess zu erfordern. Der FA ist auch für den Servicetechniker aufrufbar, um diesem eine Fehlerbehebung bei Kommunikationsproblemen zu ermöglichen.
MGMT10	▸FAKAT.SmgwAdministration	Neu: Konfigurationsmöglichkeit der Schnittstellen des SMGW ergänzt. Diese Funktionalität ist teilweise herstellerspezifisch bereits vorhanden. Die Funktion wird dem GWA und dem Servicetechniker bereitgestellt und erlaubt die Fehlerdiagnose und Behebung.
MGMT11	▸FAKAT.SmgwAdministration	Neu: Funktionalität zum Löschen aller Nutzerdaten ergänzt ("Werksreset"). Durch diese Funktion wird ein Aus- und Wiedereinbau im Sinne einer nachhaltigen Nutzung von SMGW ermöglicht. Der FA ist neben dem GWA auch für den Servicetechniker ausführbar. Dies ermöglicht die Wiederverwendung von Geräten, die kommunikativ ansonsten nicht mehr erreichbar sind und verschrottet werden müssten.
MGMT12	▸FAKAT.SmgwAdministration	Neu: Möglichkeit für GWA und Servicetechniker einen Neustart des SMGW auslösen zu können. Diese Funktion kann für eine mögliche Fehlerbehebung genutzt werden und ist in der Praxis bereits verbreitet.

Nr.	Fundstelle überarbeitete Version	Änderung im Vergleich zur Vorversion
MGMT13	▸FAKAT.GwaSwitch	Neu: der Wechselprozess für den GWA wird nun in größerem Detail beschrieben. Er orientiert sich am GWA-Wechsel gemäß FNN Mikroprozessen.
MGMT14	▸FAKAT.SmgwCertMgmt	Neu: der GWA kann nun die Zertifikate des SMGW auslesen. Diese Funktion dient der Betriebsführung und Fehlerdiagnose.
MGMT15	▸FAKAT.SmgwCertMgmt	Geändert: Funktion zum Deaktivieren bzw. Entfernen eines alten Root-CA-Zertifikats ist nun verpflichtend umzusetzen.
MGMT16	▸FAKAT.SmgwCertMgmt	Neu: Funktion zum Deaktivieren bzw. Entfernen von alten SMGW WAN-Zertifikaten ergänzt. Diese Funktion fehlte in der Vorversion, ist jedoch für die Zertifikatsverwaltung im Rahmen der Betriebsführung notwendig.
MGMT17	▸FAKAT.SmgwCertMgmt	Neu: Funktionen zur Verwaltung des Sicherheitsmodules für den GWA ergänzt. Die Funktionen und Aufrufparameter orientieren sich an den FNN Mikroprozessen.
MGMT18	▸FAKAT.SmgwFwUpdate	Geändert: Funktionalität des Firmware-Updates wurde bisher ohne nennenswerte Details gefordert. Durch FA wird nun ein interoperabler Prozess beschrieben. Funktionalität umfasst auch die Möglichkeit ein Update von kompatiblen Zähler über das SMGW auszulösen.
MGMT19	▸FAKAT.SmgwMonitoring	Neu: Auf Anforderung durch den Anschlussnutzer soll der GWA Teile des Anschlussnutzer-Logs löschen. Da diese Funktion bereits in TR-03109-6 gefordert wurde, ist sie verbindlich umzusetzen.
KS1	▸Abschnitt 4.4	Die Namen der Kommunikationsszenarien wurden wie folgt angepasst, um deren Bedeutung besser abzubilden und dem Namensschema an WAN zu folgen: • Geändert: HKS1 wird HKS.WS1 • Geändert: HKS2 wird zu HKS.WS2 • Geändert: HKS3 wird zu HKS.TLSPROXY.SOCKS • Geändert: HKS4 und 5 werden zu HKS.TLSPROXY.CLI zusammengefasst, da der Verbindungsaufbau unabhängig vom Auslöser ist • Neu: HKS.NTP-TLS.SRV als neues Kommunikationsszenario für die Bereitstellung eines Zeitservers im HAN (für TR-03109-5) • Neu: HKS.DNSDISCOVERY als neues Kommunikationsszenario zur Auflösung der Adresse und Dienste des SMGW durch HAN-Teilnehmer (für TR-03109-5)
KS2	▸Abschnitt 4.2	Neu: CMS ist nun optional in den Fällen, wo die Endpunkte für die TLS-Kommunikation und die Inhaltsdatenkommunikation identisch sind (z.B. SMGW an GWA). Bei Übertragung beispielsweise von Messwerten über den GWA an einen EMT bleibt CMS erhalten. Durch die Optionalität wird CMS nur angewendet, wenn es angefordert wird (WKS.MANAGEMENT) oder im WAN-Kommunikationsprofil entsprechend konfiguriert wurde (WKS.ADMIN-SERVICE, WKS.INFO-REPORT). Durch die Optionalität bleibt die Kompatibilität mit Altsystemen erhalten und eine Übergangsphase geboten. Gleichzeitig sorgt der Entfall von CMS in den zuvor genannten Fällen für geringeren Rechenaufwand und geringeres Datenvolumen in der WAN-Kommunikation.
KS3	▸Abschnitt 4.2	Geändert: das zuvor bereits als veraltet bezeichnete WKS.NTP-HTTPS ist entfallen und WKS.NTP-TLS ist nun verpflichtend umzusetzen.
KS4	▸Abschnitt 4.2	Neu: das neue WKS.DOWNLOAD wurde ergänzt. Der generelle Ablauf ist identisch zu WKS.ADMIN-SERVICE ohne CMS. Das neue Kommunikationsszenario erzeugt aufgrund der Ähnlichkeit kaum Implementierungsaufwand, erlaubt aber durch Entfall von CMS eine einfachere Verarbeitung und geringeres Datenvolumen, sofern dies im Backend gewünscht ist.

Nr.	Fundstelle überarbeitete Version	Änderung im Vergleich zur Vorversion
KS5	▸Abschnitt 4.3	Geändert: Aufgrund des von LKS1 abweichenden Protokollstacks, wird LKS1.PSK nun als gesondertes Kommunikationsszenario aufgeführt, statt den Aspekt des Pairings in den Anforderungen des LKS1 unterzubringen.
KS6	▸Abschnitt 4.4	Neu: Eine Differenzierung des HAN in ein Heimnetzwerk (HAN-CON) und ein Anlagennetzwerk (HAN-CLS) wurde eingeführt.
CON1	▸FAKAT.ConServices	In der FAKAT.ConServices werden Dienste für den Anschlussnutzer definiert. Die nachfolgenden Punkte geben einen Überblick und beschreiben, ob es sich um eine neue Funktion handelt oder lediglich um einen Umbau (inkl. Konkretisierung bzw. Detaillierung) einer alten Funktion auf FA-Struktur: • Umgebaut: Auslesen des Anschlussnutzer-Logs • Umgebaut: Auflisten der SMGW Ressourcen • Neu: Auslesen von Informationen über das SMGW und kommunikativ angebundene Geräte • Umgebaut: Bereitstellung des letzten empfangenen Messwerts • Umgebaut: Bereitstellung registrierter Messwerte • Umgebaut: Bereitstellung historischer Tageszählerstände • Umgebaut: Auslesen von Auswertungsprofilen • Neu: Auslesen des Status der Zeitsynchronisation und der lokalen Zeit • Neu: Auslesen der Zertifikate des SMGW • Umgebaut: Funktion zum Abmelden • Neu: Möglichkeit zur Änderung des eigenen Passworts • Neu: Bereitstellung einer Startseite für Browsernavigation
CON2	▸FAKAT.ConServices	Neu: der Anschlussnutzer kann nun die Zertifikate des SMGW auslesen. Diese Funktion dient der Transparenz gegenüber dem Anschlussnutzer. Insbesondere die Bereitstellung des Signaturzertifikats ergibt sich aus der Integration der PTB-A 50.8.
CON3	▸FAKAT.ConServices	Neu: (optional) der Anschlussnutzer kann nun sein eigenes Passwort ändern. Dies schließt eine bestehende Lücke, was im Hinblick auf die Sicherheit und Vertrauenswürdigkeit des SMGW notwendig ist. Des Weiteren vermeidet dies aufwendige Backendprozesse zur Änderung auf Veranlassung des Anschlussnutzers.
CON4	▸FAKAT.ConServices	Neu: (optional) die Anwendungsprogrammierschnittstelle dient der M2M-Kommunikation. Um dem Anschlussnutzer für die grundlegenden Funktionen eine menschenbedienbare Schnittstelle zu bieten, wird eine browserbasierte Seite vorgesehen.

Nr.	Fundstelle überarbeitete Version	Änderung im Vergleich zur Vorversion
CLS1	▸FAKAT.ClsServices	In der FAKAT.ClsServices werden Dienste für CLS-Geräte und die Proxy-Funktionen definiert. Die nachfolgenden Punkte geben einen Überblick und beschreiben, ob es sich um eine neue Funktion handelt oder lediglich um einen Umbau (inkl. Konkretisierung bzw. Detaillierung) einer alten Funktion auf FA-Struktur: • Umgebaut: TLS-Proxykanal initiiert durch CLS (bisher HKS3) • Umgebaut: TLS-Proxykanal initiiert durch den GWA (bisher HKS4) • Umgebaut: Beendigung des TLS-Proxykanals durch den GWA • Umgebaut: TLS-Proxykanal zeitgesteuert initiiert (bisher HKS5) • Neu: Bereitstellung eines Zeitsynchronisationsdienstes für CLS • Neu: Auslesen des Status des TLS-Proxykanals durch CLS • Neu: Erzeugung von Schlüsselpaaren und Zertifikaten für CLS (für TR-03109-5) Die Änderungen und neuen Funktionen dienen insbesondere dem besseren Zusammenspiel zwischen SMGW und CLS gemäß TR-03109-5.
SRV1	▸FAKAT.SrvServices	In der FAKAT.SrvServices werden Dienste für Servicetechniker definiert. Die nachfolgenden Punkte geben einen Überblick und beschreiben, ob es sich um eine neue Funktion handelt oder lediglich um einen Umbau (inkl. Konkretisierung bzw. Detailierung) einer alten Funktion auf FA-Struktur: • Umgebaut: Auslesen des System-Logs • Neu: Auslesen von Statusinformationen zu Netzwerkschnittstellen • Neu: Auflisten der SMGW Ressourcen • Umgebaut: Auslösen eines Selbsttests • Neu: Änderungen von Kommunikationsparametern für die Verbindung zum GWA (bisher HAF4) • Neu: Änderung der Schnittstellenkonfiguration für WAN, HAN und LMN (Adresse, Ports, etc.) • Neu: Auslesen der Schnittstellenkonfiguration für WAN, HAN und LMN (Adresse, Ports, etc.) • Neu: Auslesen von LMN-Kommunikationsprofilen (ehemals Zählerprofile) • Neu: Auslesen von HAN-Kommunikationsprofilen von Anschlussnutzern • Neu: Auslesen von Proxy-Kommunikationsprofilen • Neu: Auslesen des Status der Zeitsynchronisation und der lokalen Zeit • Neu: Auslesen der Zertifikate des SMGW • Neu: Löschen der Nutzerdaten ("Werksreset") • Neu: Auflistung der kommunikativ erreichbaren Messeinrichtungen • Neu: Auslesen von Informationen über das SMGW und kommunikativ angebundene Geräte • Neu: Auslösen eines Neustarts • Umgebaut: Funktion zum Abmelden Ein Großteil der Funktionen sind ausschließlich lesender Art und dienen der Fehlerdiagnose. Die auslesbaren Profile enthalten dabei keine privaten Schlüssel oder andere vertrauliche Informationen.

Nr.	Fundstelle überarbeitete Version	Änderung im Vergleich zur Vorversion
MTR1	▸FAKAT.MtrServices	In der FAKAT.MtrServices werden erweiterte Dienste für Messgeräte definiert. Die nachfolgenden Punkte geben einen Überblick und beschreiben, ob es sich um eine neue Funktion handelt oder lediglich um einen Umbau (inkl. Konkretisierung bzw. Detaillierung) einer alten Funktion auf FA-Struktur: • Neu: Auslesen von Messgeräteinformation aus der Messeinrichtung • Neu: Setzen der gesetzlichen Zeit in der Messeinrichtung • Neu: Übertragen einer Datei (Konfiguration, Update) an eine Messeinrichtung • Neu: Aufhebung der Anbindung der Messeinrichtung ans SMGW ("Crypto-Reset") Die Änderungen und neuen Funktionen dienen insbesondere der Anbindung von bzw. Interaktion mit RLM-Messeinrichtungen und Messeinrichtungen mit Konfigurations- und Updatemöglichkeit.
WFA1	-	Entfallen: es werden in der TR keine Anforderungen an die Verwendung des Sicherheitsmoduls für TLS und CMS mehr gestellt. Vorgaben an zu unterstützende und zu verwendende Algorithmen werden durch die TR-03109-3 gestellt. Die Verwendung des Sicherheitsmoduls für bestimmte Funktionalitäten (Zufallserzeugung, Signaturprüfung/-erzeugung, Schlüsselspeicher) ist bereits im PP-0073 beschrieben und im Rahmen eines Common-Criteria-Verfahrens besser überprüfbar.
WFA2	▸Kapitel 3, ▸Anhang A	Geändert und erweitert: zu protokollierende Ereignisse wurden konkretisiert und ein stärkerer Zusammenhang zu Anforderungen hergestellt. Auf die in ▸Anhang A definierten Ereignisse wird direkt aus Anforderungen verwiesen, wenn eine Protokollierung erforderlich ist. Dadurch wird die querschneidende Aktivität der Protokollierung in der TR besser abgebildet. Anforderungen, die sich rein auf die Protokollierung beziehen (ehemalige Abschnitte 5.3.1, 5.3.2 und 5.3.3) wurden aufgelöst und in stattdessen in geeigneten FA untergebracht. Die Ereignisse wurden auf Basis der vom FNN definierten Logmeldungen definiert und ggf. präzisiert. Erweiterungen wurden vorgenommen, wo dies zur Umsetzung neuer Funktionalität oder der Integration der PTB-A 50.8 Anforderungen notwendig war. Die Änderung dient der Erreichung einer besseren Interoperabilität der Ereignisse. Dadurch wird eine bessere, automatisierte Testbarkeit in Zertifizierungsverfahren sowie eine Vereinfachung der Betriebsführung erreicht.
HAN1	▸Abschnitt 4.4	Neu: Die Netzwerk-Separation des HAN in ein HAN-CON für den Endkunden und ein HAN-CLS für Anlagen wurde gemeinsam mit der Anpassung des PP-0073 eingeführt, um eine Differenzierung der Annahme an die geschützte Umgebung (OE.Network) technisch vorzubereiten.
NFA1	-	Entfallen: Anforderung an die Versiegelung des SMGW wurden entfernt, da dies bereits im Rahmen der Common Criteria (SFR FPT_PHP.1) betrachtet wird und derzeit kein Thema der Interoperabilität darstellt. Dies gilt ebenfalls für die bisher als "SOLL" geforderte aktive Gehäuseöffnungserkennung.
NFA2	▸Abschnitt 5.5	Neu/Geändert: Vorhaltefristen wurden bisher an verschiedenen Stellen der TR definiert. In Abschnitt 5.4 werden nun alle relevanten Vorhaltefristen gemäß Rechtsrahmen (MsbG und MessEG/MessEV) an zentraler Stelle übersichtlich dargestellt.
NFA3	▸Abschnitt 5.6	Neu: Abschnitt zur Leistungsfähigkeit des SMGW aufgenommen, um die 1:n-Anbindbarkeit des SMGW durch Anforderungen zu hinterlegen.

Nr.	Fundstelle überarbeitete Version	Änderung im Vergleich zur Vorversion
NFA4	▸Abschnitt 5.7	Neu: im Zusammenspiel mit dem PP-0073 in der Version von 2024 werden für die Audit Protokollierung der SFR konkrete Ereignisse vorgegeben. Dies dient der Schaffung von Interoperabilität für Testbarkeit in Zertifizierungsverfahren und im Rahmen der Betriebsführung.
NFA5	▸Kapitel 5	Neu: Im Zusammenspiel mit dem PP-0073v2.0 wird die SMGW-Einsatzumgebung "Bündelung am Netzknotenpunkt" optional vorgesehen, die Sicherheitsanforderungen bedingt.
ACC1	-	Entfallen: der ehemalige Abschnitt 4.5 (Anforderungen an Berechtigungen) ist entfallen. (Negative) Zugriffsberechtigungen lassen sich im Rahmen eines TR-Verfahrens (Black-Box-Testing) nicht hinreichend überprüfen. Des Weiteren sind Zugriffsberechtigungen bereits im PP-0073 (SFR FDP_ACF.1) definiert und im Rahmen eines Common-Criteria-Verfahrens besser prüfbar. Es wurde stattdessen ein Anhang in Abstimmung mit dem PP-0073 in der Version von 2024 erstellt (siehe anderen Eintrag).
ACC2	▸Anhang C	Neu: Anhang C wurde in Synchronisation mit dem PP-0073 in der Version von 2024 erstellt. Das PP-0073 definiert Assets und wie Rollen wie mit diesen Assets interagieren dürfen. Gemäß der Common-Criteria ist das PP dabei technologie-neutral. Die TR-03109-1 ist mit den definierten Datenstrukturen und FA wesentlich konkreter. Um die Lücke zwischen TR und PP zu schließen wurde dieser Anhang für die zulässigen Zugriffe an der HAN-Schnittstelle erstellt. Er setzt die definierten Assets und die FA in Bezug zueinander. Dies verbessert das Verständnis der Interaktion zwischen TR und PP und führt zur Vermeidung von Inkonsistenzen zwischen den Dokumenten.

Tabelle E.1 Changelog von Version 2.0 zu Version 1.1

Anforderungsverzeichnis

REQ.FA.AcceptSwitchGwa.10 151
REQ.FA.AcceptSwitchGwa.30 151
REQ.FA.CaptureRegisteredValues.10 65
REQ.FA.CaptureRegisteredValues.16 65
REQ.FA.CaptureRegisteredValues.20 65
REQ.FA.CaptureRegisteredValues.30 66
REQ.FA.CaptureRegisteredValues.40 65
REQ.FA.CaptureRequestedMtrData.10 61
REQ.FA.CaptureRequestedMtrData.20 62
REQ.FA.CaptureRequestedMtrData.30 62
REQ.FA.CaptureRequestedMtrData.40 62
REQ.FA.CaptureRequestedMtrData.51 62
REQ.FA.CaptureRequestedMtrData.75 62
REQ.FA.CaptureRequestedMtrData.80 62
REQ.FA.CaptureUnsolicitedRcvdMtrData.10 64
REQ.FA.CaptureUnsolicitedRcvdMtrData.20 64
REQ.FA.CaptureUnsolicitedRcvdMtrData.40 64
REQ.FA.CaptureUnsolictedRcvdMtrData.31 64
REQ.FA.CloseProxyCh.10 83
REQ.FA.CloseProxyCh.12 83
REQ.FA.CloseProxyCh.20 83
REQ.FA.CreateHanUserProfile.10 108
REQ.FA.CreateHanUserProfile.100 108
REQ.FA.CreateHanUserProfile.20 108
REQ.FA.CreateHanUserProfile.40 108
REQ.FA.CreateLmnComProfile.40 99
REQ.FA.CreateLmnComProfile.41 99
REQ.FA.CreateLmnComProfile.50 99
REQ.FA.CreateLmnComProfile.80 99
REQ.FA.CreateNdsConfig.10 173
REQ.FA.CreateNdsConfig.11 173
REQ.FA.CreateNdsConfig.30 173
REQ.FA.CreateNdsConfig.40 173
REQ.FA.CreateProcessingProfile.10 114
REQ.FA.CreateProcessingProfile.15 114

REQ.FA.CreateProcessingProfile.260 114
REQ.FA.CreateProcessingProfile.30 114
REQ.FA.CreateProcessingProfile.50 115
REQ.FA.CreateProcessingProfile.60 114
REQ.FA.CreateProcessingProfile.70 115
REQ.FA.CreateProxyConfig.10 121
REQ.FA.CreateProxyConfig.100 121
REQ.FA.CreateProxyConfig.15 122
REQ.FA.CreateProxyConfig.16 122
REQ.FA.CreateProxyConfig.20 122
REQ.FA.CreateProxyConfig.50 122
REQ.FA.CreateWanComProfile.10 137
REQ.FA.CreateWanComProfile.20 137
REQ.FA.CreateWanComProfile.30 137
REQ.FA.CreateWanComProfile.50 137
REQ.FA.DeleteFwUpdateConfig.10 168
REQ.FA.DeleteFwUpdateConfig.20 168
REQ.FA.DeleteHanUserProfile.10 110
REQ.FA.DeleteHanUserProfile.20 110
REQ.FA.DeleteHanUserProfile.30 110
REQ.FA.DeleteLmnComProfile.10 101
REQ.FA.DeleteLmnComProfile.11 101
REQ.FA.DeleteLmnComProfile.20 101
REQ.FA.DeleteLmnComProfile.30 101
REQ.FA.DeleteNdsConfig.10 174
REQ.FA.DeleteNdsConfig.20 174
REQ.FA.DeleteNdsConfig.30 174
REQ.FA.DeleteProcessingProfile.10 119
REQ.FA.DeleteProcessingProfile.20 120
REQ.FA.DeleteProcessingProfile.30 120
REQ.FA.DeleteProcessingProfile.40 119
REQ.FA.DeleteProxyConfig.10 123
REQ.FA.DeleteProxyConfig.20 123
REQ.FA.DeleteProxyConfig.30 123
REQ.FA.DeleteWanComProfile.10 139
REQ.FA.DeleteWanComProfile.20 139

REQ.FA.DoChangeUserPassword.10 74
REQ.FA.DoChangeUserPassword.20 74
REQ.FA.DoChangeUserPassword.30 74
REQ.FA.DoChangeUserPassword.40 74
REQ.FA.DoChangeUserPassword.50 74
REQ.FA.DoCreateKeyPairAndClsCert.10 84
REQ.FA.DoCreateKeyPairAndClsCert.20 84
REQ.FA.DoCreateKeyPairAndClsCert.30 84
REQ.FA.DoCreateKeyPairAndClsCert.31 84
REQ.FA.DoCreateKeyPairAndClsCert.40 84
REQ.FA.DoCreateKeyPairAndClsCert.50 84
REQ.FA.DoCreateSelfsignedSmgwHanCert.10 160
REQ.FA.DoCreateSelfsignedSmgwHanCert.20 160
REQ.FA.DoCreateSelfsignedSmgwHanCert.30 160
REQ.FA.DoCreateSelfsignedSmgwHanCert.40 160
REQ.FA.DoCreateSelfsignedSmgwLmnCert.10 161
REQ.FA.DoCreateSelfsignedSmgwLmnCert.20 161
REQ.FA.DoCreateSelfsignedSmgwLmnCert.30 161
REQ.FA.DoCreateSelfsignedSmgwLmnCert.40 161
REQ.FA.DoDeactivateGwaCerts.10 144
REQ.FA.DoDeactivateGwaCerts.15 144
REQ.FA.DoDeactivateGwaCerts.20 144
REQ.FA.DoDeactivateGwaCerts.30 144
REQ.FA.DoDeactivateRootCaCert.10 154
REQ.FA.DoDeactivateRootCaCert.20 154
REQ.FA.DoDeactivateRootCaCert.30 154
REQ.FA.DoDeactivateRootCaCert.40 154
REQ.FA.DoDeactivateRootCaCert.50 154
REQ.FA.DoDeactivateSelfsignedSmgwHanCert.10 161
REQ.FA.DoDeactivateSelfsignedSmgwHanCert.30 161
REQ.FA.DoDeactivateSelfsignedSmgwHanCert.40 161
REQ.FA.DoDeactivateSelfsignedSmgwLmnCert.10 162
REQ.FA.DoDeactivateSelfsignedSmgwLmnCert.20 162
REQ.FA.DoDeactivateSelfsignedSmgwLmnCert.30 162
REQ.FA.DoDeactivateSelfsignedSmgwLmnCert.40 162
REQ.FA.DoDeactivateSmgwPkiCerts.10 158

REQ.FA.DoDeactivateSmgwPkiCerts.12 158
REQ.FA.DoDeactivateSmgwPkiCerts.20 158
REQ.FA.DoDeactivateSmgwPkiCerts.30 158
REQ.FA.DoDeleteUserData.10 148
REQ.FA.DoDeleteUserData.20 148
REQ.FA.DoDeleteUserData.30 148
REQ.FA.DoDeleteUserData.40 149
REQ.FA.DoEventNotification.10 126
REQ.FA.DoExportSmgwLmnCertToMtr.10 103
REQ.FA.DoExportSmgwLmnCertToMtr.20 103
REQ.FA.DoExportSmgwLmnCertToMtr.30 103
REQ.FA.DoFinishSecmodAuth.10 146
REQ.FA.DoFinishSecmodAuth.20 147
REQ.FA.DoFwActivation.10 166
REQ.FA.DoFwActivation.20 166
REQ.FA.DoFwActivation.25 166
REQ.FA.DoFwActivation.40 166
REQ.FA.DoFwActivation.5 166
REQ.FA.DoFwActivation.50 166
REQ.FA.DoFwActivation.60 166
REQ.FA.DoFwDownload.10 165
REQ.FA.DoFwDownload.20 165
REQ.FA.DoFwDownload.30 165
REQ.FA.DoFwDownload.40 165
REQ.FA.DoFwDownload.50 165
REQ.FA.DoFwDownload.60 165
REQ.FA.DoFwDownload.70 165
REQ.FA.DoImportGwaKeys.10 143
REQ.FA.DoImportGwaKeys.20 143
REQ.FA.DoImportGwaKeys.30 143
REQ.FA.DoImportRootCaCert.15 153
REQ.FA.DoImportRootCaCert.60 153
REQ.FA.DoImportRootCaCert.70 153
REQ.FA.DoImportRootCaCert.80 153
REQ.FA.DoImportSmgwPkiCerts.20 157
REQ.FA.DoImportSmgwPkiCerts.30 157

REQ.FA.DoImportSmgwPkiCerts.50 157
REQ.FA.DoImportSmgwPkiCerts.60 157
REQ.FA.DoInitialMtrSmgwPairing.10 102
REQ.FA.DoInitialMtrSmgwPairing.20 102
REQ.FA.DoInitialMtrSmgwPairing.30 102
REQ.FA.DoInitialMtrSmgwPairing.40 102
REQ.FA.DoInitialMtrSmgwPairing.50 102
REQ.FA.DoInitialMtrSmgwPairing.60 102
REQ.FA.DoInitialMtrSmgwPairing.70 102
REQ.FA.DoLogout.10 75
REQ.FA.DoLogout.20 75
REQ.FA.DoLogout.30 75
REQ.FA.DoNdsNotification.10 170
REQ.FA.DoNdsNotification.100 171
REQ.FA.DoNdsNotification.110 172
REQ.FA.DoNdsNotification.120 172
REQ.FA.DoNdsNotification.130 170
REQ.FA.DoNdsNotification.140 170
REQ.FA.DoNdsNotification.150 170
REQ.FA.DoNdsNotification.160 171
REQ.FA.DoNdsNotification.170 171
REQ.FA.DoNdsNotification.180 171
REQ.FA.DoNdsNotification.190 171
REQ.FA.DoNdsNotification.20 170
REQ.FA.DoNdsNotification.200 171
REQ.FA.DoNdsNotification.220 172
REQ.FA.DoNdsNotification.230 172
REQ.FA.DoNdsNotification.30 170
REQ.FA.DoNdsNotification.40 172
REQ.FA.DoNdsNotification.50 172
REQ.FA.DoNdsNotification.60 172
REQ.FA.DoNdsNotification.70 170
REQ.FA.DoNdsNotification.90 171
REQ.FA.DoOnDemandDelivery.10 56
REQ.FA.DoOnDemandDelivery.100 57
REQ.FA.DoOnDemandDelivery.11 56

REQ.FA.DoOnDemandDelivery.110 56
REQ.FA.DoOnDemandDelivery.120 57
REQ.FA.DoOnDemandDelivery.20 56
REQ.FA.DoOnDemandDelivery.30 56
REQ.FA.DoOnDemandDelivery.50 56
REQ.FA.DoOnDemandDelivery.55 57
REQ.FA.DoOnDemandDelivery.60 57
REQ.FA.DoOnDemandDelivery.70 57
REQ.FA.DoOnDemandDelivery.80 56
REQ.FA.DoOnDemandDelivery.90 56
REQ.FA.DoPrepareImportGwaKeys.10 143
REQ.FA.DoPrepareImportGwaKeys.20 143
REQ.FA.DoPrepareImportRootCaKey.10 163
REQ.FA.DoPrepareImportRootCaKey.20 163
REQ.FA.DoPrepareSecmod.10 162
REQ.FA.DoPrepareSecmod.20 162
REQ.FA.DoReboot.10 147
REQ.FA.DoReboot.20 147
REQ.FA.DoRemoveSmgwAssocInMtr.10 89
REQ.FA.DoRemoveSmgwAssocInMtr.12 90
REQ.FA.DoRemoveSmgwAssocInMtr.13 90
REQ.FA.DoRemoveSmgwAssocInMtr.20 90
REQ.FA.DoRemoveSmgwAssocInMtr.30 89
REQ.FA.DoRenewMtrCertificate.10 104
REQ.FA.DoRenewMtrCertificate.20 103
REQ.FA.DoReqExportHistoricReadings.10 57
REQ.FA.DoReqExportHistoricReadings.20 57
REQ.FA.DoReqExportHistoricReadings.40 58
REQ.FA.DoReqExportHistoricReadings.50 58
REQ.FA.DoReqExportHistoricReadings.70 58
REQ.FA.DoReqExportHistoricReadings.80 57
REQ.FA.DoReqExportHistoricReadings.90 58
REQ.FA.DoRequestSecmodAuth.10 144
REQ.FA.DoRequestSecmodAuth.20 144
REQ.FA.DoRequestSecmodAuth.30 144
REQ.FA.DoRequestWanComTest.10 140

REQ.FA.DoRequestWanComTest.20 140
REQ.FA.DoResetTamperState.10 90
REQ.FA.DoResetTamperState.20 90
REQ.FA.DoResetTamperState.30 90
REQ.FA.DoResponseSecmodAuth.10 146
REQ.FA.DoResponseSecmodAuth.20 146
REQ.FA.DoResponseSecmodAuth.30 146
REQ.FA.DoResponseSecmodAuth.50 146
REQ.FA.DoResponseSecmodAuth.55 146
REQ.FA.DoResponseSecmodAuth.60 145
REQ.FA.DoSelftest.10 131
REQ.FA.DoSmgwPkiCertRequest.10 155
REQ.FA.DoSmgwPkiCertRequest.15 155
REQ.FA.DoSmgwPkiCertRequest.16 156
REQ.FA.DoSmgwPkiCertRequest.20 156
REQ.FA.DoSmgwPkiCertRequest.30 156
REQ.FA.DoSmgwPkiCertRequest.40 156
REQ.FA.DoSmgwPkiCertRequest.42 156
REQ.FA.DoSmgwPkiCertRequest.44 156
REQ.FA.DoSmgwPkiCertRequest.50 156
REQ.FA.DoSmgwPkiCertRequest.60 155
REQ.FA.DoSwitchGwa.10 150
REQ.FA.DoSwitchGwa.20 150
REQ.FA.DoSwitchGwa.30 150
REQ.FA.DoSwitchGwa.40 150
REQ.FA.DoSwitchGwa.50 150
REQ.FA.DoSwitchGwa.60 150
REQ.FA.DoTruncateCalLog.10 135
REQ.FA.DoTruncateCalLog.20 135
REQ.FA.DoTruncateCalLog.30 135
REQ.FA.DoTruncateCalLog.40 135
REQ.FA.DoTruncateCalLog.50 135
REQ.FA.EventLog.10 130
REQ.FA.EventLog.20 130
REQ.FA.ExportAccntMtrReading.10 51
REQ.FA.ExportAccntMtrReading.100 52

REQ.FA.ExportAccntMtrReading.110 52
REQ.FA.ExportAccntMtrReading.120 52
REQ.FA.ExportAccntMtrReading.130 52
REQ.FA.ExportAccntMtrReading.140 52
REQ.FA.ExportAccntMtrReading.150 52
REQ.FA.ExportAccntMtrReading.20 51
REQ.FA.ExportAccntMtrReading.25 51
REQ.FA.ExportAccntMtrReading.30 51
REQ.FA.ExportAccntMtrReading.40 52
REQ.FA.ExportAccntMtrReading.41 52
REQ.FA.ExportAccntMtrReading.70 52
REQ.FA.ExportAccntMtrReading.90 52
REQ.FA.ExportCalLog.10 127
REQ.FA.ExportCalLog.100 127
REQ.FA.ExportCalLog.20 127
REQ.FA.ExportCalLog.30 127
REQ.FA.ExportCalLog.40 127
REQ.FA.ExportCalLog.50 127
REQ.FA.ExportCalLog.60 127
REQ.FA.ExportCalLog.70 127
REQ.FA.ExportCalLog.80 128
REQ.FA.ExportCalLog.90 128
REQ.FA.ExportDailyMtrReading.20 73
REQ.FA.ExportDailyMtrReading.30 73
REQ.FA.ExportDailyMtrReading.50 73
REQ.FA.ExportDailyMtrReading.60 73
REQ.FA.ExportDailyMtrReading.70 73
REQ.FA.ExportDailyMtrReading.80 73
REQ.FA.ExportDailyMtrReading.90 73
REQ.FA.ExportDerivedMtrReading.10 77
REQ.FA.ExportDerivedMtrReading.30 77
REQ.FA.ExportDerivedMtrReading.40 77
REQ.FA.ExportDerivedMtrReading.50 77
REQ.FA.ExportDerivedMtrReading.60 77
REQ.FA.ExportDerivedMtrReading.70 77
REQ.FA.ExportDerivedMtrReading.80 77

REQ.FA.ExportDerivedMtrReading.90 77
REQ.FA.ExportFileToMtr.10 88
REQ.FA.ExportFileToMtr.20 88
REQ.FA.ExportFileToMtr.30 88
REQ.FA.ExportNonAccntMtrReading.10 54
REQ.FA.ExportNonAccntMtrReading.20 55
REQ.FA.ExportNonAccntMtrReading.25 55
REQ.FA.ExportNonAccntMtrReading.30 55
REQ.FA.ExportNonAccntMtrReading.40 55
REQ.FA.ExportNonAccntMtrReading.50 55
REQ.FA.ExportNonAccntMtrReading.60 55
REQ.FA.ExportRegMtrReading.100 71
REQ.FA.ExportRegMtrReading.20 71
REQ.FA.ExportRegMtrReading.30 72
REQ.FA.ExportRegMtrReading.40 72
REQ.FA.ExportRegMtrReading.50 72
REQ.FA.ExportRegMtrReading.60 71
REQ.FA.ExportRegMtrReading.70 72
REQ.FA.ExportRegMtrReading.80 72
REQ.FA.ExportSysLog.10 126
REQ.FA.ExportSysLog.100 126
REQ.FA.ExportSysLog.20 126
REQ.FA.ExportSysLog.40 126
REQ.FA.ExportSysLog.50 126
REQ.FA.ExportSysLog.60 126
REQ.FA.ExportSysLog.70 126
REQ.FA.ExportSysLog.80 126
REQ.FA.ExportSysLog.90 126
REQ.FA.ExportTimeToMtr.10 88
REQ.FA.ExportTimeToMtr.20 88
REQ.FA.ExportUserLog.10 69
REQ.FA.ExportUserLog.100 69
REQ.FA.ExportUserLog.110 69
REQ.FA.ExportUserLog.120 68
REQ.FA.ExportUserLog.20 69
REQ.FA.ExportUserLog.30 69

REQ.FA.ExportUserLog.31 69
REQ.FA.ExportUserLog.40 69
REQ.FA.ExportUserLog.50 69
REQ.FA.ExportUserLog.60 69
REQ.FA.ExportUserLog.70 69
REQ.FA.ExportUserLog.80 69
REQ.FA.ExportUserLog.90 69
REQ.FA.InitiateManagementConnection.10 147
REQ.FA.ListIdentifiedCls.10 112
REQ.FA.ListIdentifiedCls.20 112
REQ.FA.ListIdentifiedCls.30 112
REQ.FA.ListIdentifiedCls.40 112
REQ.FA.ListIdentifiedCls.50 112
REQ.FA.ListIdentifiedMeters.10 105
REQ.FA.ListIdentifiedMeters.20 105
REQ.FA.ListIdentifiedMeters.30 105
REQ.FA.ListIdentifiedMeters.40 105
REQ.FA.ListIdentifiedMeters.50 105
REQ.FA.ListSmgwResources.10 132
REQ.FA.ListSmgwResources.20 132
REQ.FA.MeteringValidation.10 30
REQ.FA.MeteringValidation.60 30
REQ.FA.NotifySystemEvents.10 125
REQ.FA.NtpTimeService.20 97
REQ.FA.NtpTimeService.30 97
REQ.FA.NtpTimeService.40 98
REQ.FA.NtpTimeService.50 98
REQ.FA.NtpTimeService.60 98
REQ.FA.NtpTimeService.70 98
REQ.FA.NtpTimeService.80 98
REQ.FA.ReadCertificate.20 159
REQ.FA.ReadCertificate.30 159
REQ.FA.ReadDeviceInfo.10 132
REQ.FA.ReadDeviceInfo.20 133
REQ.FA.ReadDeviceInfo.30 133
REQ.FA.ReadDeviceInfo.40 133

REQ.FA.ReadDeviceInfoFromMtr.10 89
REQ.FA.ReadDeviceInfoFromMtr.20 89
REQ.FA.ReadDeviceInfoFromMtr.30 89
REQ.FA.ReadDeviceStatus.10 133
REQ.FA.ReadDeviceStatus.15 133
REQ.FA.ReadDeviceStatus.20 133
REQ.FA.ReadDeviceStatus.30 133
REQ.FA.ReadDeviceStatus.40 133
REQ.FA.ReadFwUpdateConfig.10 167
REQ.FA.ReadFwUpdateConfig.20 167
REQ.FA.ReadHanIfProfile.10 129
REQ.FA.ReadHanIfProfile.20 129
REQ.FA.ReadHanUserProfile.10 111
REQ.FA.ReadHanUserProfile.20 111
REQ.FA.ReadInstantMtrReading.10 70
REQ.FA.ReadInstantMtrReading.15 70
REQ.FA.ReadInstantMtrReading.20 70
REQ.FA.ReadInstantMtrReading.25 70
REQ.FA.ReadInstantMtrReading.30 70
REQ.FA.ReadInstantMtrReading.40 70
REQ.FA.ReadInstantMtrReading.50 70
REQ.FA.ReadInstantMtrReading.60 70
REQ.FA.ReadLmnComProfile.10 101
REQ.FA.ReadLmnComProfile.20 101
REQ.FA.ReadLmnIfProfile.10 129
REQ.FA.ReadLmnIfProfile.20 129
REQ.FA.ReadNdsConfig.10 174
REQ.FA.ReadNdsConfig.20 174
REQ.FA.ReadNetworkIfStatus.10 128
REQ.FA.ReadNetworkIfStatus.20 128
REQ.FA.ReadNetworkIfStatus.30 128
REQ.FA.ReadNotificationProfile.10 134
REQ.FA.ReadNotificationProfile.20 134
REQ.FA.ReadProcessingProfile.10 120
REQ.FA.ReadProcessingProfile.20 120
REQ.FA.ReadProxyChStatus.10 83

REQ.FA.ReadProxyChStatus.20 84
REQ.FA.ReadProxyChStatus.30 84
REQ.FA.ReadProxyChStatus.40 84
REQ.FA.ReadProxyChStatus.50 84
REQ.FA.ReadProxyConfig.10 124
REQ.FA.ReadProxyConfig.20 123
REQ.FA.ReadSecmodState.10 163
REQ.FA.ReadSecmodState.20 163
REQ.FA.ReadStartPage.10 76
REQ.FA.ReadStartPage.20 76
REQ.FA.ReadStartPage.30 76
REQ.FA.ReadStartPage.40 76
REQ.FA.ReadStartPage.50 76
REQ.FA.ReadStartPage.60 76
REQ.FA.ReadStartPage.70 76
REQ.FA.ReadStartPage.80 76
REQ.FA.ReadTariffState.10 78
REQ.FA.ReadTariffState.30 78
REQ.FA.ReadTariffState.40 79
REQ.FA.ReadTariffState.50 78
REQ.FA.ReadTimeSyncStatus.10 97
REQ.FA.ReadTimeSyncStatus.20 97
REQ.FA.ReadTimeSyncStatus.30 97
REQ.FA.ReadWanComProfile.10 140
REQ.FA.ReadWanComProfile.20 140
REQ.FA.ReadWanIfProfile.10 129
REQ.FA.ReadWanIfProfile.20 129
REQ.FA.RequestProxyCh.10 82
REQ.FA.RequestProxyCh.20 82
REQ.FA.RequestProxyCh.30 82
REQ.FA.RequestProxyCh.40 82
REQ.FA.RequestProxyCh.50 82
REQ.FA.RequestProxyChByCls.10 81
REQ.FA.RequestProxyChByCls.20 82
REQ.FA.RequestProxyChByCls.30 81
REQ.FA.RequestProxyChByCls.40 81

REQ.FA.RequestProxyChByCls.50 81
REQ.FA.RequestProxyChByCls.60 82
REQ.FA.RetrieveClockStateFromMtr.10 91
REQ.FA.RetrieveClockStateFromMtr.20 91
REQ.FA.RetrieveClockStateFromMtr.30 91
REQ.FA.RetrieveFileFromMtr.10 91
REQ.FA.RetrieveFileFromMtr.20 91
REQ.FA.RetrieveFileFromMtr.30 91
REQ.FA.SyncTimeWithGwa.10 94
REQ.FA.SyncTimeWithGwa.20 95
REQ.FA.UpdateFwUpdateConfig.20 167
REQ.FA.UpdateFwUpdateConfig.30 167
REQ.FA.UpdateFwUpdateConfig.40 167
REQ.FA.UpdateFwUpdateConfig.5 167
REQ.FA.UpdateHanIfProfile.10 142
REQ.FA.UpdateHanIfProfile.20 141
REQ.FA.UpdateHanIfProfile.30 141
REQ.FA.UpdateHanIfProfile.40 141
REQ.FA.UpdateHanIfProfile.45 141
REQ.FA.UpdateHanUserProfile.10 110
REQ.FA.UpdateHanUserProfile.20 110
REQ.FA.UpdateHanUserProfile.40 110
REQ.FA.UpdateHanUserProfile.50 110
REQ.FA.UpdateHanUserProfile.80 109
REQ.FA.UpdateHanUserProfile.90 110
REQ.FA.UpdateLmnComProfile.10 100
REQ.FA.UpdateLmnComProfile.15 100
REQ.FA.UpdateLmnComProfile.16 100
REQ.FA.UpdateLmnComProfile.30 100
REQ.FA.UpdateLmnComProfile.60 100
REQ.FA.UpdateLmnIfProfile.10 142
REQ.FA.UpdateLmnIfProfile.20 142
REQ.FA.UpdateLmnIfProfile.30 142
REQ.FA.UpdateNdsConfig.10 174
REQ.FA.UpdateNdsConfig.11 174
REQ.FA.UpdateNdsConfig.20 174

REQ.FA.UpdateNdsConfig.30 174
REQ.FA.UpdateNotificationProfile.10 134
REQ.FA.UpdateNotificationProfile.20 134
REQ.FA.UpdateNotificationProfile.30 134
REQ.FA.UpdateProcessingProfile.15 119
REQ.FA.UpdateProcessingProfile.20 118
REQ.FA.UpdateProcessingProfile.60 118
REQ.FA.UpdateProcessingProfile.80 119
REQ.FA.UpdateProcessingProfile.90 118
REQ.FA.UpdateProxyConfig.10 123
REQ.FA.UpdateProxyConfig.100 122
REQ.FA.UpdateProxyConfig.20 123
REQ.FA.UpdateProxyConfig.25 123
REQ.FA.UpdateProxyConfig.30 123
REQ.FA.UpdateWanComProfile.10 138
REQ.FA.UpdateWanComProfile.20 138
REQ.FA.UpdateWanComProfile.30 138
REQ.FA.UpdateWanComProfile.45 138
REQ.FA.UpdateWanComProfile.50 138
REQ.FA.UpdateWanIfProfile.10 141
REQ.FA.UpdateWanIfProfile.20 141
REQ.FA.UpdateWanIfProfile.25 141
REQ.FA.UpdateWanIfProfile.30 140
REQ.FAKAT.ClsServices.10 80
REQ.FAKAT.ClsServices.100 80
REQ.FAKAT.ClsServices.110 80
REQ.FAKAT.ClsServices.120 80
REQ.FAKAT.ClsServices.130 80
REQ.FAKAT.ClsServices.140 80
REQ.FAKAT.ClsServices.150 80
REQ.FAKAT.ClsServices.30 80
REQ.FAKAT.ClsServices.50 80
REQ.FAKAT.ClsServices.60 80
REQ.FAKAT.ClsServices.70 80
REQ.FAKAT.ClsServices.80 80
REQ.FAKAT.ClsServices.90 80

REQ.FAKAT.ConServices.100 67
REQ.FAKAT.ConServices.20 67
REQ.FAKAT.ConServices.30 67
REQ.FAKAT.ConServices.40 67
REQ.FAKAT.ConServices.50 67
REQ.FAKAT.ConServices.60 67
REQ.FAKAT.ConServices.70 67
REQ.FAKAT.ConServices.80 67
REQ.FAKAT.ConServices.90 67
REQ.FAKAT.EmtComConfig.30 106
REQ.FAKAT.EmtComConfig.40 106
REQ.FAKAT.FwDownload.20 199
REQ.FAKAT.FwDownload.30 164
REQ.FAKAT.FwDownload.40 164
REQ.FAKAT.FwDownload.50 164
REQ.FAKAT.GwaSwitch.20 150
REQ.FAKAT.HanUserConfig.20 107
REQ.FAKAT.HanUserConfig.30 107
REQ.FAKAT.LmnComConfig.20 98
REQ.FAKAT.MeteringConfig.10 113
REQ.FAKAT.MeteringConfig.20 113
REQ.FAKAT.MeteringConfig.30 113
REQ.FAKAT.MeteringConfig.50 113
REQ.FAKAT.MeteringConfig.70 217
REQ.FAKAT.MeteringConfig.80 50
REQ.FAKAT.MeteringConfig.90 50
REQ.FAKAT.MtrServices.10 87
REQ.FAKAT.MtrServices.20 87
REQ.FAKAT.MtrServices.30 87
REQ.FAKAT.MtrServices.40 87
REQ.FAKAT.MtrServices.50 87
REQ.FAKAT.MtrServices.60 87
REQ.FAKAT.NetworkDiagnosis.30 213
REQ.FAKAT.NetworkDiagnosis.50 171
REQ.FAKAT.NetworkDiagnosis.60 171
REQ.FAKAT.NetworkDiagnosis.70 215

REQ.FAKAT.ProxyConfig.20 121
REQ.FAKAT.ProxyConfig.30 121
REQ.FAKAT.SmgwAdministration.10 136
REQ.FAKAT.SmgwAdministration.100 136
REQ.FAKAT.SmgwAdministration.70 136
REQ.FAKAT.SmgwAdministration.80 136
REQ.FAKAT.SmgwAdministration.90 136
REQ.FAKAT.SmgwCertMgmt.20 195
REQ.FAKAT.SmgwCertMgmt.50 192
REQ.FAKAT.SmgwCertMgmt.60 223
REQ.FAKAT.SmgwMonitoring.10 124
REQ.FAKAT.SmgwMonitoring.100 125
REQ.FAKAT.SmgwMonitoring.11 124
REQ.FAKAT.SmgwMonitoring.31 210
REQ.FAKAT.SmgwMonitoring.50 124
REQ.FAKAT.SmgwMonitoring.60 124
REQ.FAKAT.SmgwMonitoring.80 124
REQ.FAKAT.SmgwMonitoring.90 125
REQ.FAKAT.SmgwOperation.110 169
REQ.FAKAT.SmgwOperation.130 124
REQ.FAKAT.SmgwOperation.140 124
REQ.FAKAT.SmgwOperation.150 124
REQ.FAKAT.SmgwOperation.160 124
REQ.FAKAT.SmgwOperation.170 124
REQ.FAKAT.SmgwOperation.200 124
REQ.FAKAT.SmgwOperation.60 164
REQ.FAKAT.SrvServices.10 85
REQ.FAKAT.SrvServices.100 86
REQ.FAKAT.SrvServices.110 86
REQ.FAKAT.SrvServices.120 86
REQ.FAKAT.SrvServices.130 86
REQ.FAKAT.SrvServices.140 86
REQ.FAKAT.SrvServices.150 86
REQ.FAKAT.SrvServices.160 86
REQ.FAKAT.SrvServices.170 85
REQ.FAKAT.SrvServices.180 86

REQ.FAKAT.SrvServices.190 ... 86
REQ.FAKAT.SrvServices.20 ... 86
REQ.FAKAT.SrvServices.30 ... 86
REQ.FAKAT.SrvServices.40 ... 86
REQ.FAKAT.SrvServices.50 ... 86
REQ.FAKAT.SrvServices.60 ... 86
REQ.FAKAT.SrvServices.70 ... 86
REQ.FAKAT.SrvServices.80 ... 86
REQ.FAKAT.SrvServices.90 ... 86
REQ.FAKAT.ValCapture.10 ... 59
REQ.FAKAT.ValCapture.20 ... 59
REQ.FAKAT.ValCapture.21 ... 59
REQ.FAKAT.ValCapture.30 ... 59
REQ.FAKAT.ValCapture.40 ... 60
REQ.FAKAT.ValCapture.50 ... 60
REQ.FAKAT.ValProcBilling.10 ... 27
REQ.FAKAT.ValProcBilling.20 ... 27
REQ.FAKAT.ValProcBilling.30 ... 27
REQ.FAKAT.ValProcBilling.40 ... 27
REQ.FAKAT.ValProcBilling.50 ... 27
REQ.FAKAT.ValProcBilling.60 ... 27
REQ.FAKAT.ValProcBilling.Accumulation.10 ... 34
REQ.FAKAT.ValProcBilling.Accumulation.20 ... 34
REQ.FAKAT.ValProcBilling.Accumulation.30 ... 34
REQ.FAKAT.ValProcBilling.Accumulation.40 ... 34
REQ.FAKAT.ValProcBilling.DerivePower.10 ... 37
REQ.FAKAT.ValProcBilling.DerivePower.20 ... 37
REQ.FAKAT.ValProcBilling.DerivePower.25 ... 37
REQ.FAKAT.ValProcBilling.DerivePower.30 ... 37
REQ.FAKAT.ValProcBilling.DerivePower.40 ... 37
REQ.FAKAT.ValProcBilling.DerivePower.50 ... 37
REQ.FAKAT.ValProcBilling.Registration.10 ... 29
REQ.FAKAT.ValProcBilling.Registration.100 ... 30
REQ.FAKAT.ValProcBilling.Registration.120 ... 30
REQ.FAKAT.ValProcBilling.Registration.130 ... 30
REQ.FAKAT.ValProcBilling.Registration.30 ... 30

REQ.FAKAT.ValProcBilling.Registration.40 30
REQ.FAKAT.ValProcBilling.Registration.50 30
REQ.FAKAT.ValProcBilling.Registration.55 30
REQ.FAKAT.ValProcBilling.Registration.80 29
REQ.FAKAT.ValProcBilling.Registration.90 30
REQ.FAKAT.ValProcBilling.Registration.91 30
REQ.FAKAT.ValProcDaily.Capturing.10 32
REQ.FAKAT.ValProcDaily.Capturing.30 32
REQ.FAKAT.ValProcDaily.Capturing.50 32
REQ.FAKAT.ValProcDaily.Capturing.60 32
REQ.FAKAT.ValProcNonBilling.10 46
REQ.FAKAT.ValProcNonBilling.20 46
REQ.FAKAT.ValProcNonBilling.30 46
REQ.FAKAT.ValProcNonBilling.40 46
REQ.FAKAT.ValProcNonBilling.Capturing.10 46
REQ.FAKAT.ValProcNonBilling.Capturing.30 46
REQ.FAKAT.ValProcNonBilling.Capturing.40 47
REQ.FAKAT.ValProcNonBilling.Capturing.50 47
REQ.FAKAT.ValProcNonBilling.Capturing.60 47
REQ.FAKAT.ValProcNonBilling.Capturing.70 47
REQ.HAN.AnschlussnutzerDatenbereitstellung.10 66
REQ.HAN.AnschlussnutzerDatenbereitstellung.120 66
REQ.HAN.AnschlussnutzerDatenbereitstellung.30 66
REQ.HAN.AnschlussnutzerDatenbereitstellung.40 67
REQ.HAN.AnschlussnutzerDatenbereitstellung.50 66
REQ.HAN.AnschlussnutzerDatenbereitstellung.70 67
REQ.HAN.AnschlussnutzerDatenbereitstellung.71 73
REQ.HAN.HKS1.11 272
REQ.HAN.HKS1.20 272
REQ.HAN.HKS1.50 272
REQ.HAN.HKS1.60 272
REQ.HAN.HKS2.21 274
REQ.HAN.HKS2.23 275
REQ.HAN.HKS2.30 275
REQ.HAN.HKS2.60 275
REQ.HAN.HKS3.70 79

REQ.HAN.HKS4.10 82
REQ.HAN.HKS4.21 282
REQ.HAN.HKS4.30 82
REQ.HAN.HKS4.40 282
REQ.HAN.HKS4.41 282
REQ.HAN.HKS4.50 252
REQ.HAN.HKS5.60 80
REQ.HAN.Kommunikationsprofile.20 268
REQ.HAN.Kommunikationsprofile.30 205
REQ.HAN.Kommunikationsprofile.60 268
REQ.HAN.Kommunikationsszenarien.20 266
REQ.HAN.Kommunikationsszenarien.22 266
REQ.HAN.Kommunikationsszenarien.30 266
REQ.HAN.Kommunikationsszenarien.40 266
REQ.HAN.Kommunikationsszenarien.50 266
REQ.HAN.Kommunikationsszenarien.60 266
REQ.HAN.Kommunikationsszenarien.61 266
REQ.HAN.Network.30 269
REQ.HAN.Network.40 269
REQ.HAN.Network.70 269
REQ.HAN.PhysSchnittstelle.10 269
REQ.HAN.PhysSchnittstelle.20 269
REQ.HAN.PhysSchnittstelle.30 269
REQ.HAN.PhysSchnittstelle.40 269
REQ.HAN.PhysSchnittstelle.55 269
REQ.HAN.PhysSchnittstelle.61 269
REQ.HAN.PhysSchnittstelle.71 269
REQ.HAN.PhysSchnittstelle.80 269
REQ.HAN.ProxyKommunikationsprofile.20 220
REQ.HAN.ServiceTechnikerDatenbereitstellung.10 85
REQ.HAN.ServiceTechnikerDatenbereitstellung.20 85
REQ.HAN.ServiceTechnikerDatenbereitstellung.30 85
REQ.HAN.ServiceTechnikerGwaKommunikation.10 85
REQ.HAN.ServiceTechnikerGwaKommunikation.20 86
REQ.HAN.ServiceTechnikerSelbsttest.10 85
REQ.HAN.SicherungKommunikation.20 267

REQ.HAN.SicherungKommunikation.21 267
REQ.HAN.SicherungKommunikation.22 267
REQ.HAN.SicherungKommunikation.40 267
REQ.HAN.SicherungKommunikation.41 267
REQ.HAN.SicherungKommunikation.50 267
REQ.HAN.SicherungKommunikation.60 267
REQ.HAN.SicherungKommunikationConSrv.20 67
REQ.HAN.SicherungKommunikationConSrv.21 86
REQ.HAN.SicherungKommunikationConSrv.70 275
REQ.HAN.Transport.70 268
REQ.HAN.Transport.80 268
REQ.HAN.Webservice.10 272
REQ.HAN.Webservice.11 275
REQ.HAN.Webservice.20 272
REQ.HAN.Webservice.30 272
REQ.HAN.Webservice.70 272
REQ.HAN.Webservice.71 272
REQ.HAN.Webservice.72 272
REQ.HAN.Webservice.73 275
REQ.HKS.DNS.SRV.10 285
REQ.HKS.DNS.SRV.20 285
REQ.HKS.DNS.SRV.30 285
REQ.HKS.DNS.SRV.40 285
REQ.HKS.DNS.SRV.5 285
REQ.HKS.DNS.SRV.50 285
REQ.HKS.DNSDISCOVERY.10 285
REQ.HKS.DNSDISCOVERY.20 285
REQ.HKS.NTP-TLS.SRV.10 283
REQ.HKS.NTP-TLS.SRV.20 283
REQ.HKS.NTP-TLS.SRV.30 284
REQ.HKS.NTP-TLS.SRV.50 283
REQ.HKS.TLSPROXY.CLI.10 282
REQ.HKS.TLSPROXY.CLI.20 282
REQ.HKS.TLSPROXY.CLI.30 282
REQ.HKS.TLSPROXY.SOCKS.10 278
REQ.HKS.TLSPROXY.SOCKS.20 278

REQ.HKS.TLSPROXY.SOCKS.30 278
REQ.HKS.TLSPROXY.SRV.10 280
REQ.HKS.TLSPROXY.SRV.20 280
REQ.HKS.TLSPROXY.SRV.30 280
REQ.HKS.WS1.10 271
REQ.HKS.WS1.20 272
REQ.HKS.WS1.21 272
REQ.HKS.WS2.10 274
REQ.HKS.WS2.21 275
REQ.LMN.Anwendungsprotokolle.10 257
REQ.LMN.Anwendungsprotokolle.20 257
REQ.LMN.Anwendungsprotokolle.30 257
REQ.LMN.Kommunikationsprotokolle.10 258
REQ.LMN.Kommunikationsprotokolle.11 258
REQ.LMN.Kommunikationsprotokolle.20 265
REQ.LMN.Kommunikationsprotokolle.30 265
REQ.LMN.Kommunikationsprotokolle.40 260
REQ.LMN.Kommunikationsprotokolle.41 263
REQ.LMN.Kommunikationsprotokolle.42 260
REQ.LMN.Kommunikationsprotokolle.50 260
REQ.LMN.Kommunikationsprotokolle.51 260
REQ.LMN.LKS1.10 260
REQ.LMN.LKS1.20 260
REQ.LMN.LKS1.30 260
REQ.LMN.LKS1.40 260
REQ.LMN.LKS1.50 260
REQ.LMN.LKS1.PSK.10 263
REQ.LMN.LKS1.PSK.30 263
REQ.LMN.LKS2.10 265
REQ.LMN.LKS2.20 265
REQ.LMN.LKS2.30 265
REQ.LMN.LKS2.40 265
REQ.LMN.Messwertempfang.20 58
REQ.LMN.Messwertempfang.30 58
REQ.LMN.Messwertempfang.50 58
REQ.LMN.Sicherung.10 257

REQ.LMN.TlsSicherung.70 104
REQ.LMN.Zaehlerverwaltung.20 98
REQ.LMN.Zaehlerverwaltung.30 98
REQ.LMN.Zaehlerverwaltung.40 98
REQ.LMN.Zaehlerverwaltung.60 87
REQ.MWV.Pseudonymisierung.10 55
REQ.MWV.Zählerprofil.20 208
REQ.NFA.ArchiveDuration.10 286
REQ.NFA.AuditEvents.10 288
REQ.NFA.AuditEvents.20 288
REQ.NFA.AuditEvents.30 288
REQ.NFA.Einbau.10 286
REQ.NFA.Einbau.20 286
REQ.NFA.Performance.10 287
REQ.Profile.10 175
REQ.WAF2.Zeitsynchronisation.20 95
REQ.WAF2.Zeitsynchronisation.30 95
REQ.WAF2.Zeitsynchronisation.50 95
REQ.WAF2.Zeitsynchronisation.51 95
REQ.WAF2.Zeitsynchronisation.52 92
REQ.WAF2.Zeitsynchronisation.53 95
REQ.WAF2.Zeitsynchronisation.54 95
REQ.WAF2.Zeitsynchronisation.55 95
REQ.WAF2.Zeitsynchronisation.60 95
REQ.WAN.CmsSicherung.30 240
REQ.WAN.CmsSicherung.31 240
REQ.WAN.Datenmodell.10 16
REQ.WAN.EmtBenachrichtigung.10 49
REQ.WAN.EmtBenachrichtigung.20 49
REQ.WAN.EmtBenachrichtigung.40 170
REQ.WAN.GwaBenachrichtigung.10 124
REQ.WAN.Kommunikationsprofil.20 231
REQ.WAN.Kommunikationsprofil.41 237
REQ.WAN.Kommunikationsprofil.60 139
REQ.WAN.Kommunikationsszenarien.100 82
REQ.WAN.Kommunikationsszenarien.110 147

REQ.WAN.Kommunikationsszenarien.30 236
REQ.WAN.Kommunikationsszenarien.40 236
REQ.WAN.Kommunikationsszenarien.50 236
REQ.WAN.Kommunikationsszenarien.51 236
REQ.WAN.Kommunikationsszenarien.70 125
REQ.WAN.Kommunikationsszenarien.90 95
REQ.WAN.Management.10 98
REQ.WAN.Management.100 80
REQ.WAN.Management.11 98
REQ.WAN.Management.110 80
REQ.WAN.Management.140 106
REQ.WAN.Management.150 106
REQ.WAN.Management.160 136
REQ.WAN.Management.161 136
REQ.WAN.Management.162 136
REQ.WAN.Management.172 152
REQ.WAN.Management.175 152
REQ.WAN.Management.180 152
REQ.WAN.Management.181 152
REQ.WAN.Management.182 151
REQ.WAN.Management.190 136
REQ.WAN.Management.191 149
REQ.WAN.Management.193 151
REQ.WAN.Management.195 136
REQ.WAN.Management.196 152
REQ.WAN.Management.197 152
REQ.WAN.Management.20 98
REQ.WAN.Management.200 152
REQ.WAN.Management.201 152
REQ.WAN.Management.202 152
REQ.WAN.Management.210 152
REQ.WAN.Management.220 152
REQ.WAN.Management.230 149
REQ.WAN.Management.231 149
REQ.WAN.Management.250 164
REQ.WAN.Management.260 136

REQ.WAN.Management.272 92
REQ.WAN.Management.273 92
REQ.WAN.Management.280 124
REQ.WAN.Management.290 124
REQ.WAN.Management.30 98
REQ.WAN.Management.300 169
REQ.WAN.Management.301 169
REQ.WAN.Management.302 169
REQ.WAN.Management.303 169
REQ.WAN.Management.310 124
REQ.WAN.Management.40 107
REQ.WAN.Management.41 107
REQ.WAN.Management.50 107
REQ.WAN.Management.80 121
REQ.WAN.Management.81 121
REQ.WAN.Management.90 121
REQ.WAN.Selbsttest.10 131
REQ.WAN.Selbsttest.20 131
REQ.WAN.Selbsttest.21 131
REQ.WAN.Selbsttest.40 99
REQ.WAN.Selbsttest.70 131
REQ.WAN.Selbsttest.80 131
REQ.WAN.TlsSicherung.40 237
REQ.WAN.TlsSicherung.60 236
REQ.WAN.TlsSicherung.80 236
REQ.WAN.Transport.20 237
REQ.WAN.Transport.30 237
REQ.WAN.Transport.31 238
REQ.WAN.Transport.50 236
REQ.WAN.Transport.51 237
REQ.WAN.Transport.60 238
REQ.WAN.Transport.70 237
REQ.WAN.Transport.80 237
REQ.WAN.Transport.81 237
REQ.WAN.Transport.90 237
REQ.WAN.WakeUp.10 136

REQ.WAN.WAKEUP.20 254
REQ.WAN.WakeUpSicherung.10 253
REQ.WAN.WakeUpSicherung.20 253
REQ.WAN.WakeUpSicherung.30 253
REQ.WAN.WakeUpSicherung.40 253
REQ.WAN.WakeUpSicherung.50 253
REQ.WAN.WakeUpSicherung.60 253
REQ.WAN.WakeUpSicherung.80 253
REQ.WAN.Webservice.10 240
REQ.WAN.Webservice.100 241
REQ.WAN.Webservice.110 241
REQ.WAN.Webservice.120 240
REQ.WAN.Webservice.130 241
REQ.WAN.Webservice.20 240
REQ.WAN.Webservice.50 247
REQ.WAN.Webservice.60 240
REQ.WAN.Webservice.70 240
REQ.WAN.Webservice.90 240
REQ.WAN.Zeitsynchronisation.10 250
REQ.WAN.Zeitsynchronisation.100 95
REQ.WAN.Zeitsynchronisation.110 95
REQ.WAN.Zeitsynchronisation.40 250
REQ.WAN.Zeitsynchronisation.70 249
REQ.WAN.Zeitsynchronisation.80 95
REQ.WAN.ZugriffAufGwaDienste.10 92
REQ.WAN.ZugriffAufGwaDienste.20 164
REQ.WAN.ZugriffAufGwaDienste.30 50
REQ.WAN.ZugriffAufGwaDienste.40 50
REQ.WAN.ZugriffAufGwaDienste.50 170
REQ.WFA.AnLog.20 286
REQ.WFA.EichLog.10 286
REQ.WFA.EichlogInhalt.40 115
REQ.WFA.EichlogInhalt.41 119
REQ.WFA.Logformat.40 130
REQ.WFA.Logformat.50 130
REQ.WFA.SMGW-ID.10 286

REQ.WFA.SMGW-ID.20 286
REQ.WFA.SysLog.10 286
REQ.WFA.SysLogInhalt.10 124
REQ.WFA.SysLogInhalt.20 125
REQ.WFA.SysLogInhalt.30 125
REQ.WKS.ADMIN-SERVICE.10 243
REQ.WKS.ADMIN-SERVICE.100 243
REQ.WKS.ADMIN-SERVICE.110 244
REQ.WKS.ADMIN-SERVICE.20 243
REQ.WKS.ADMIN-SERVICE.30 243
REQ.WKS.ADMIN-SERVICE.31 243
REQ.WKS.ADMIN-SERVICE.40 243
REQ.WKS.ADMIN-SERVICE.50 243
REQ.WKS.ADMIN-SERVICE.51 243
REQ.WKS.ADMIN-SERVICE.60 243
REQ.WKS.ADMIN-SERVICE.70 243
REQ.WKS.ADMIN-SERVICE.80 243
REQ.WKS.DOWNLOAD.10 255
REQ.WKS.DOWNLOAD.100 256
REQ.WKS.DOWNLOAD.20 255
REQ.WKS.DOWNLOAD.30 256
REQ.WKS.DOWNLOAD.40 256
REQ.WKS.DOWNLOAD.50 255
REQ.WKS.DOWNLOAD.60 256
REQ.WKS.DOWNLOAD.80 256
REQ.WKS.INFO-REPORT.10 246
REQ.WKS.INFO-REPORT.100 248
REQ.WKS.INFO-REPORT.20 247
REQ.WKS.INFO-REPORT.30 247
REQ.WKS.INFO-REPORT.31 247
REQ.WKS.INFO-REPORT.40 248
REQ.WKS.INFO-REPORT.50 247
REQ.WKS.INFO-REPORT.51 247
REQ.WKS.INFO-REPORT.52 248
REQ.WKS.INFO-REPORT.53 248
REQ.WKS.INFO-REPORT.60 248

REQ.WKS.INFO-REPORT.70 247
REQ.WKS.INFO-REPORT.90 248
REQ.WKS.MANAGEMENT.10 239
REQ.WKS.MANAGEMENT.20 240
REQ.WKS.MANAGEMENT.30 240
REQ.WKS.MANAGEMENT.40 240
REQ.WKS.MANAGEMENT.50 241
REQ.WKS.MANAGEMENT.60 240
REQ.WKS.MANAGEMENT.70 241
REQ.WKS.MANAGEMENT.90 241
REQ.WKS.NTP-TLS.10 249
REQ.WKS.NTP-TLS.20 249
REQ.WKS.NTP-TLS.30 249
REQ.WKS.TLS-PROXY.10 251
REQ.WKS.TLS-PROXY.20 252
REQ.WKS.TLS-PROXY.30 252
REQ.WKS.TLS-PROXY.40 252
REQ.WKS.WAKEUP.10 253
REQ.WKS.WakeUp.20 147
REQ.WKS.WAKEUP.30 253

ICS-Verzeichnis

ICS.FA.CaptureRequestedMtrData.10 62
ICS.FA.CaptureUnsolicitedRcvdMtrData.10 64
ICS.FA.CaptureUnsolicitedRcvdMtrData.20 64
ICS.FA.CloseProxyCh.10 83
ICS.FA.CreateHanUserProfile.10 109
ICS.FA.CreateLmnComProfile.10 100
ICS.FA.CreateLmnComProfile.20 100
ICS.FA.CreateLmnComProfile.30 100
ICS.FA.CreateProcessingProfile.30 118
ICS.FA.CreateProcessingProfile.40 118
ICS.FA.CreateProcessingProfile.50 118
ICS.FA.CreateProxyConfig.10 122
ICS.FA.CreateWanComProfile.10 138
ICS.FA.DoChangeUserPassword.10 74

ICS.FA.DoDeleteUserData.10 149
ICS.FA.DoFwActivation.10 166
ICS.FA.DoFwActivation.20 167
ICS.FA.DoFwDownload.10 165
ICS.FA.DoFwDownload.20 165
ICS.FA.DoFwDownload.30 165
ICS.FA.DoImportRootCaCert.10 154
ICS.FA.DoImportSmgwPkiCerts.10 158
ICS.FA.DoInitialMtrSmgwPairing.10 103
ICS.FA.DoOnDemandDelivery.10 57
ICS.FA.DoReboot.10 148
ICS.FA.DoRenewMtrCertificate.10 104
ICS.FA.DoSelftest.10 132
ICS.FA.EventLog.10 130
ICS.FA.EventLog.20 130
ICS.FA.EventLog.30 131
ICS.FA.EventLog.40 131
ICS.FA.ExportAccntMtrReading.10 53
ICS.FA.ExportCalLog.10 128
ICS.FA.ExportCalLog.20 128
ICS.FA.ExportCalLog.30 128
ICS.FA.ExportDailyMtrReading.10 74
ICS.FA.ExportDerivedMtrReading.10 77
ICS.FA.ExportDerivedMtrReading.20 78
ICS.FA.ExportRegMtrReading.10 72
ICS.FA.ExportRegMtrReading.20 72
ICS.FA.ExportSysLog.10 127
ICS.FA.ExportSysLog.80 127
ICS.FA.ExportUserLog.10 69
ICS.FA.ListIdentifiedCls.10 112
ICS.FA.ListIdentifiedMeters.10 105
ICS.FA.ListIdentifiedMeters.20 105
ICS.FA.NtpTimeService.10 98
ICS.FA.ReadCertificate.20 159
ICS.FA.ReadInstantMtrReading.10 70
ICS.FA.ReadInstantMtrReading.20 71

ICS.FA.ReadInstantMtrReading.40 71
ICS.FA.RetrieveFileFromMtr.20 91
ICS.FA.TimeSyncWithGwa.60 96
ICS.FA.TimeSyncWithGwa.70 96
ICS.FA.TimeSyncWithGwa.80 96
ICS.FA.TimeSyncWithGwa.90 96
ICS.FA.UpdateHanIfProfile.10 142
ICS.FAKAT.ClsServices.10 80
ICS.FAKAT.ClsServices.30 81
ICS.FAKAT.ConServices.10 67
ICS.FAKAT.EmtComConfig.10 106
ICS.FAKAT.FwDownload.10 199
ICS.FAKAT.FwDownload.30 164
ICS.FAKAT.HanUserConfig.10 107
ICS.FAKAT.LmnComConfig.10 99
ICS.FAKAT.MeteringConfig.10 217
ICS.FAKAT.MtrServices.10 87
ICS.FAKAT.NetworkDiagnosis.10 213
ICS.FAKAT.NetworkDiagnosis.20 215
ICS.FAKAT.ProxyConfig.10 121
ICS.FAKAT.SmgwAdministration.10 136
ICS.FAKAT.SmgwCertMgmt.10 152
ICS.FAKAT.SmgwCertMgmt.20 195
ICS.FAKAT.SmgwCertMgmt.30 192
ICS.FAKAT.SmgwCertMgmt.40 223
ICS.FAKAT.SmgwMonitoring.10 196
ICS.FAKAT.SmgwMonitoring.20 125
ICS.FAKAT.SmgwMonitoring.31 210
ICS.FAKAT.SmgwMonitoring.32 210
ICS.FAKAT.SmgwTimeSync.40 92
ICS.FAKAT.SrvServices.200 87
ICS.FAKAT.ValProcBilling.10 27
ICS.FAKAT.ValProcBilling.20 27
ICS.FAKAT.ValProcBilling.Registration.10 31
ICS.FAKAT.ValProcDaily.10 32
ICS.FAKAT.ValProcDaily.20 33

ICS.FAKAT.ValProcNonBilling.10 46
ICS.FAKAT.ValProcNonBilling.Capturing.10 47
ICS.FAKAT.ValProcNonBilling.Capturing.20 47
ICS.FAKAT.ValTransmission.10 50
ICS.HAN.IfProfile.10 201
ICS.HAN.Kommunikationsprofile.10 205
ICS.HAN.Kommunikationsszenarien.10 269
ICS.HAN.PhysSchnittstelle.10 270
ICS.HAN.PhysSchnittstelle.40 270
ICS.HAN.ProxyKommunikationsprofile.10 220
ICS.HAN.ServiceTechnikerDatenbereitstellung.10 128
ICS.HAN.SicherungKommunikation.10 268
ICS.HAN.SicherungKommunikationConSrv.10 67
ICS.HAN.SicherungKommunikationConSrv.40 272
ICS.HAN.SicherungKommunikationConSrv.50 201
ICS.HAN.SicherungKommunikationConSrv.60 201
ICS.HAN.SicherungKommunikationConSrv.70 272
ICS.HAN.SicherungKommunikationConSrv.80 273
ICS.LMN.IfProfile.10 206
ICS.LMN.Sicherung.10 258
ICS.MWV.MwStatus.10 31
ICS.MWV.Taf14Obis.10 118
ICS.MWV.Zählerprofil.10 208
ICS.NDS.Lebenszyklus.10 169
ICS.NDS.Schwellwerte.10 172
ICS.NDS.Umsetzung.10 169
ICS.NDS.Uri.20 172
ICS.NDS.Uri.21 172
ICS.NDS.Uri.30 173
ICS.NDS.Uri.31 173
ICS.NDS.Versand.10 172
ICS.NFA.AuditEvents.10 288
ICS.NFA.Performance.20 288
ICS.WAF2.Zeitsynchronisation.10 96
ICS.WAF2.Zeitsynchronisation.20 96
ICS.WAF2.Zeitsynchronisation.30 96

ICS.WAF2.Zeitsynchronisation.40 96
ICS.WAF2.Zeitsynchronisation.50 96
ICS.WAN.IfProfile.10 227
ICS.WAN.Kommunikationsprofil.10 231
ICS.WAN.Kommunikationsprofil.20 231
ICS.WAN.Kommunikationsprofil.50 231
ICS.WAN.Selbsttest.30 99
ICS.WAN.Transport.20 238
ICS.WAN.Transport.30 238
ICS.WAN.Transport.40 238
ICS.WAN.WakeUpSicherung.10 254
ICS.WFA.SysLogSpannungsausfall.10 125
ICS.WKS.ADMIN-SERVICE.10 244
ICS.WKS.ADMIN-SERVICE.20 244
ICS.WKS.INFO-REPORT.10 248
ICS.WKS.INFO-REPORT.20 248
ICS.WKS.MANAGEMENT.10 241
ICS.WKS.MANAGEMENT.20 241
ICS.ZertifikateHAN.Allgemein.20 268
ICS.ZertifikateHAN.Allgemein.30 160