Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

TR-03109-1 Detailspezifikationen

Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems

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

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

Inhaltsverzeichnis

1. Einleitung

Die folgenden Kapitel enthalten die Detailspezifikationen zur Technischen Richtlinie BSI TR-03109-1.

Die Detailspezifikationen dieses Dokumentes setzen die Anwendungsfälle und Kommunikationsszenarien des SMGW um und ergänzen deren Anforderungen um Detailanforderungen.

Zielgruppe dieses Dokumentes sind daher die Geräteentwickler des Herstellers des SMGW und die für den Test des SMGW zuständigen Stellen.

Die in diesem Dokument enthaltenen Spezifikationen referenzieren in der Regel Universalspezifikationen oder Teile davon und können weitere anwendungsspezifische Anforderungen enthalten. Universalspezifikationen sind beispielsweise Normen, Standards, Richtlinien des BSI, der IETF und weiterer nationaler, europäischer oder internationaler Normungsorganisationen.

Die in diesem Dokument enthaltenen, einzelnen Kapitel widmen sich unterschiedlichsten Bereichen. Sie sind daher nicht zur zusammenhängenden Lektüre gedacht.

2. Datenstruktur der Wake-Up-Nachricht

Die Wake-Up-Nachricht enthält insbesondere

- die Identifikation zum Aufbau der Datenstruktur und zur Bedeutung der Datenfelder
- die Geräteidentifikation des SMGW
- einen Zeitstempel des Absenders
- die Signatur des Absenders

Das SMGW **MUSS** Wake-Up-Nachrichten mit folgender Struktur und Bedeutung verarbeiten können: [REQ.WakeUp.Datenstruktur.10]

Feld	#Bytes	Beschreibung
Header	2	Header = „WU“ (ASCII “57h 55h” = “0101.0111b 0101.0101b”). Dient zur Kennzeichnung der Wake-Up-Nachricht und ermöglicht eine erste einfache (hardwarenahe) Überprüfung bzw. Klassifizierung der empfangenen Nachrichten.
VersionId	1	Wake-Up-Nachricht Version = 01h. Bezeichnet die verwendete Version des Wake-Up-Protokolles. Bei eventuellen zukünftigen Erweiterungen werden neue Versionsnummern vergeben.
RecipientId	9	Eineindeutige Geräte-Identifikation des SMGW. Kodierung gemäß [DIN43863-5] Byte[1]: Sparte (01h..0Fh): 0Eh=Kommunikation Byte[2-4]: Herstellerkennzeichnung (3 ASCII Großbuchstaben) gemäß FLAG Registrierung. Zum Beispiel: „BSI“ 42 53 49h Die Kodierung erfolgt beginnend mit dem höchstwertigen Byte. Byte[5]: Fabrikationsblock (00h..FEh) Byte[6-9]: Fabrikationsnummer rechtsbündig mit führenden Nullen (8 Dezimalstellen 0000 0000 - 9999 9999). Die Kodierung erfolgt als 32 Bit Unsigned Integer und beginnend mit dem höchstwertigen Byte. Dient zur eindeutigen Identifizierung des SMGW. Die Vergabe und Bedeutung der RecipientId ist in [DIN43863-5] beschrieben.[1]
Timestamp	8	UTC Unix Time als 64 Bit Signed Integer (Anzahl Sekunden seit dem 1. Januar 1970 00:00:00 UTC). Zum Beispiel: „13. Juli 2012 11:01:20 UTC“ „1.342.177.280d“ = „00 00 00 00 50 00 00 00h“ Die Kodierung erfolgt beginnend mit dem niederwertigen Byte. Enthält die aktuelle Zeit (in UTC) zum Zeitpunkt der Erstellung der Wake-Up-Nachricht. Geringfügige Unterschiede zwischen den jeweiligen Uhrzeiten auf den Servern und den SMGW sind üblich. Das SMGW prüft, ob der Timestamp im festgelegten Zeitfenster relativ zur Uhrzeit des SMGW liegt. Der Timestamp dient dazu, dass eine einzelne Wake-Up-Nachricht nicht mehrfach für den Aufbau von TLS-Verbindungen wiederverwendet werden kann (Replay-Attacke).
Padding / Reserved	12	Zwölf mal "0Bh"

[1] Nur das adressierte SMGW darf die Wake-Up-Nachricht verarbeiten. Hiermit soll verhindert werden, dass die Wake-Up-Nachricht von einem Angreifer missbraucht wird, um eine Vielzahl von SMGW in der Verantwortung eines GWA zu einem gleichzeitigen TLS-Callback zu verleiten (DoS-Attacke).

Feld	#Bytes	Beschreibung
SignatureFormat	1	Dient zur Kennzeichnung welches Signaturformat in der Wake-Up-Nachricht verwendet wurde. Plain Format = 01h
SignatureAlgorithmOIDLength	1	Länge des folgenden SignatureAlgorithmObjectIdentifiers.
SignatureAlgorithmOID	1..14	OID des verwendeten Signaturalgorithmus gemäß [TR-03109-3] ohne Padding Zum Beispiel: ecdsa-plain-SHA256 ::= { itu-t(0) identified-organization(4) etsi(0) reserved(127) etsi-identified-organization(0) bsi-de(7) algorithms(1) id-ecc(1) signatures(4) ecdsa-plain-signatures(1) 3 }
Signature	**2*L**	Signatur R||S über die Datenfelder "Header" bis "Padding" inklusive. Octet string R = I2OS(**r**; **L**) und S = I2OS(**s**; **L**) Die Länge **L** bestimmt sich aus der elliptischen Kurve des öffentlichen Signaturschlüssels zum GWA_WAN_SIG_CRT.

Tabelle 2.1 Datenstruktur der Wake-Up-Nachricht

Das SMGW **MUSS** den Hash über die Datenfelder "Header" bis einschließlich "Padding" nach [TR-03111] Kap 4.1.2.1 mit dem öffentlichen Schlüssel des GWA_WAN_SIG_CRT validieren. [REQ.WakeUp.Datenstruktur.20]

Das SMGW **MUSS** für die Validierung der Signatur das über **SignatureAlgorithmOID** bestimmte Hash- und Signaturverfahren gemäß [TR-03109-3] und die durch den öffentlichen Signaturschlüssel des GWA_WAN_SIG_CRT bestimmte elliptische Kurve verwenden. [REQ.WakeUp.Datenstruktur.30]

Die in ▸Tabelle 2.1 abgebildete Struktur wird als Wake-Up-Nachricht an das SMGW versendet.

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

Tabelle 2.2 Struktur Wake-Up-Nachricht

3. Zertifikatsprofile am LMN

3.1. Einleitung

Die selbstsignierten LMN-Zertifikate, die das SMGW erstellt und verwendet, verwenden die Syntax und Semantik von X.509-Zertifikaten in der Version 3 nach [RFC5280] Kapitel 4 und **SOLLEN** konform zu dem in diesem Kapitel beschriebenen Zertifikatsprofil sein. [REQ.ZertifikateLMN.Allgemein.10]

ICS.ZertifikateLMN.Allgemein.10

Der Hersteller **MUSS** im ICS deklarieren, ob das SMGW die Anforderungen an die LMN-Zertifikatsprofile für MTR und SMGW für die vom SMGW erzeugten und verarbeiteten LMN-Zertifikate umsetzt und die Abweichungen in einer Anlage zum ICS beschreiben.

Zertifikatstyp	Zertifikats-Profiltyp	Aussteller
GW_LMN_TLS_CRT	Selbst-Signiert	SMGW
MTR_LMN_TLS_CRT	Selbst-Signiert	SMGW

Tabelle 3.1 Zertifikatsprofiltypen der LMN-Zertifikate

Die folgenden Abschnitte enthalten Tabellen in denen Anforderungen an das Vorhandensein von Attributen und Datenfelder verschiedener Zertifikatsprofile beschrieben sind. Darin werden die folgenden Abkürzungen verwendet:

Zeichen	Langform	Bedeutung
m	Mandatory	Das Element muss vorhanden sein.
x	Not existent	Das Element darf nicht vorhanden sein.
o	Optional	Das Element kann vorhanden sein
c	Conditional	Das Element ist abhängig von einem anderen Element vorhanden
r	Recommended	Das Element soll vorhanden sein.

Tabelle 3.2 Beschreibung der Abkürzung zum Vorhandensein von Zertifikats-Elementen

3.2. Laufzeit

Die Laufzeit der selbstsignierten LMN-Zertifikate ist in [TR-03109-3] beschrieben.

3.3. Zertifikatsstruktur

Zertifikatsfeld	Referenz in RFC5280	Element vorhanden	Wert
TBSCertificate	4.1.1.1	m	Siehe ▸Tabelle 3.4
SignatureAlgorithm	4.1.1.2	m	Siehe ▸Abschnitt 3.3.1
SignatureValue	4.1.1.3	m	Abhängig vom gewählten Signatur-Algorithmus. Mit dem privaten Schlüssel zum "subjectPublicKeyInfo" selbstsigniert.

Zertifikatsfeld	Referenz in RFC5280	Element vorhanden	Wert
Größe von Certificate		r	<=600 Bytes.

Tabelle 3.3 Struktur des Elementes "Certificate"

Die folgende Tabelle gibt die Struktur des Feldes "TBSCertificate" verbindlich vor.

Zertifikatsfeld	Referenz in RFC5280	Element vorhanden	Wert
Version	4.1.2.1	m	'v3'
SerialNumber	4.1.2.2	m	Zufällig gewählte, positive Ganzzahl; bestimmt vom Aussteller (8-20 Octets).
Signature	4.1.2.3	m	Gleicher Wert wie im Feld "SignatureAlgorithm" (s. ▸Abschnitt 3.3.1).
Issuer	4.1.2.4	m	Identisch zu "Subject".
Validity	4.1.2.5	m	Zeitpunkte für Beginn und Ende der Gültigkeit des Zertifikates (s. ▸Abschnitt 3.3.4).
Subject	4.1.2.6	m	Eindeutiger Name (Distinguished Name, DN) des Zertifikatsinhabers siehe ▸Abschnitt 3.3.3.
SubjectPublicKeyInfo	4.1.2.7	m	Siehe ▸Abschnitt 3.3.2.
IssuerUniqueId	4.1.2.8	x	Entfällt
SubjectUniqueId	4.1.2.8	x	Entfällt
Extensions	4.1.2.9	m	Siehe ▸Abschnitt 3.3.5.

Tabelle 3.4 Struktur des Elementes "TBSCertificate"

3.3.1. SignatureAlgorithm

Durch die Datenstruktur SignatureAlgorithm wird nach [RFC5280] der Signaturalgorithmus des Zertifikats angegeben. Dieser besteht aus der folgenden Datenstruktur:

```
AlgorithmIdentifier ::= SEQUENCE {algorithm OBJECT IDENTIFIER, parameters ANY DEFINED BY algorithm OPTIONAL}
```

Der Wert von "algorithm" wird - angelehnt an die Vorgaben für Sub-CA nach [TR-03116-3] Tabelle 4 - mit ECDSA-with-SHA256 oder ECDSA-with-SHA384 angegeben. Das Datenfeld "parameters" bleibt leer.

3.3.2. SubjectPublicKeyInfo

Das Feld "SubjectPublicKeyInfo" besitzt folgende Struktur (s. [RFC5480]):

```
SubjectPublicKeyInfo ::= SEQUENCE {algorithm AlgorithmIdentifier, subjectPublicKey BIT STRING}
```

Die OID im Datenfeld "algorithm" enthält den Wert 1.2.840.10045.2.1 (id-ecPublicKey). Im Feld "ECParameters" ist gemäß [RFC5480] die Variante namedCurve zu verwenden. Für die aktuell zu verwendenden Werte siehe [TR-03116-3] Kapitel 6.2.

Der PublicKey wird mit unkomprimierten Punktkoordinaten angegeben.

3.3.3. Issuer und Subject

- Für selbstsignierte LMN-Zertifikate sind "subject" und "issuer" identisch.
- Einzelne Attribute von Issuer und Subject dürfen nicht länger als 64 Zeichen sein.

- Es wird zwischen den Funktionsrollen SMGW und MTR unterschieden.
- Die LMN-Zertifikate (SMGW und MTR) stammen nicht aus der SM-PKI.
- Vorgaben an das Namensschema von Issuer und Subject sind in ▸Abschnitt 3.5 und ▸Abschnitt 3.4 beschrieben.

3.3.4. Validity

- Das Feld "notBefore" enthält den Erzeugungszeitpunkt des Schlüsselpaares und des Zertifikates.
- Das Feld "notAfter" enthält den Zeitpunkt, nach dem das Zertifikat und das dazugehörige Schlüsselpaar nicht mehr verwendet werden darf. Der Zeitpunkt darf nicht nach dem Ende des Gültigkeitszeitraumes nach [TR-03116-3] Tabelle 10 liegen.

3.3.5. Extensions

Die nun folgende Tabelle enthält eine Übersicht der Extensions und den Anforderungen an deren Vorhandensein. Weitere Zertifikats-Extensions sind nicht erlaubt.

Nr.	Bezeichnung	MTR_LMN_TLS_CRT Element vorhanden	GW_LMN_TLS_CRT Element vorhanden
1	AuthorityKeyIdentifier	x	x
2	SubjectKeyIdentifier	o	o
3	KeyUsage	r	r
4	PrivateKeyUsagePeriod	x	x
5	CertificatePolicies	x	x
6	SubjectAltNames	c (siehe ▸Abschnitt 3.3.5.3	c (siehe ▸Abschnitt 3.3.5.3)
7	IssuerAltName	x	x
8	BasicConstraints	r	r
9	ExtendedKeyUsage	r[1]	r[1]
10	CRLDistributionPoints	x	x

Tabelle 3.5 Extensions

3.3.5.1. KeyUsage

- Extension-ID (OID): 2.5.29.15
- Kritisch: Ja
- Beschreibung: Die Extension KeyUsage (spezifiziert in [RFC5280], 4.2.1.1) definiert, für welche Zwecke der zertifizierte öffentliche Schlüssel verwendet werden darf.
- Gesetzte Bits: digitalSignature(0)

3.3.5.2. BasicConstraints

- Extension-ID (OID): 2.5.29.19
- Kritisch: Nein
- Beschreibung: Diese Extension (spezifiziert in [RFC5280], 4.2.1.9) gibt an, ob es sich bei dem gegebenen Zertifikat um eine CA handelt und wie viele CAs ihr folgen können.
- "cA": FALSE

[1] Für die Verwendung mit id-kp-serverAuth und id-kp-clientAuth

3.3.5.3. SubjectAltName

- Extension-ID (OID): 2.5.29.27
- Kritisch: Ja
- Beschreibung: Diese Extension (spezifiziert in [RFC5280], 4.2.1.6) ermöglicht die Bindung von Identitäten an das Subject des Zertifikates. Diese Angabe ist alternativ oder zusätzlich zur Identifikation im Subject möglich.
- "dNSName": Es wird empfohlen, die eindeutige Kennung von SMGW oder der Messeinrichtung basierend auf [DIN43863-5] als Domain Name Label mit angehängtem ".sm" zu formatieren.

3.4. Anforderungen an die LMN-TLS-Zertifikate der Messeinrichtungen

3.4.1. Einleitung

Zusätzlich zu den Anforderungen nach ▸Abschnitt 3.3 gelten für *MTR_LMN_TLS_CRT*-Zertifikate die Anforderungen in ▸Abschnitt 3.4.

3.4.2. Issuer und Subject

Für Zertifikate der Messeinrichtung gilt für die Bildung des *SubjectCN* die Bildungsregel <id>.<idscheme>:

- Die Identifikation (<id>) enthält die herstellerübergreifende Identifikationsnummer für Messeinrichtungen nach [DIN43863-5] mit der Sparte "1" (Elektrizität), "5" (Kälte), "6" (Wärme), "7" (Gas), "8" (Kaltwasser), oder "9" (Heißwasser).
- Das Identifikationsschema (<idscheme>) enthält den Text "sm"
- Der *SubjectCN* ist Case-insensitiv zu interpretieren.

3.5. Anforderungen an die LMN-TLS-Zertifikate des SMGW

3.5.1. Einleitung

Zusätzlich zu den Anforderungen nach ▸Abschnitt 3.3 gelten für *GW_LMN_TLS_CRT*-Zertifikate die Anforderungen in ▸Abschnitt 3.5.

3.5.2. Issuer und Subject

Für Gateway-Zertifikate gilt für die Bildung des *SubjectCN* die Bildungsregel <id>.<idscheme>:

- Die Identifikation (<id>) enthält die herstellerübergreifende Identifikationsnummer für Messeinrichtungen nach [DIN43863-5] mit der Sparte "E".
- Das Identifikationsschema (<idscheme>) enthält den Text "sm"
- Der *SubjectCN* ist Case-insensitiv zu interpretieren.

3.5.3. Beispiel

```
Certificate:
 Data:
  Version: 3 (0x2)
  Serial Number: e8:a5:fe:ee:52:36:de:56
  Signature Algorithm: ecdsa-with-SHA256
  Issuer: CN = ebsi0012345678.sm
  Validity
```

```
            Not Before: Jul  1 00:00:00 2018 GMT
            Not After : Jul  1 00:00:00 2025 GMT
          Subject: CN = ebsi0012345678.sm
          Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
            Public-Key: (256 bit)
              pub: 04:0c:fa:22:10:64:6d:05:c9:ff:ab:91:71:86:ca:
                   94:3b:6a:08:8e:f7:78:ab:a0:3c:4f:fe:22:48:97:
                   71:18:6e:13:dd:c2:bd:47:19:cf:2b:58:16:a3:d5:
                   fc:7d:57:b8:02:63:71:47:f2:c7:36:f7:5d:51:b5:
                   bf:ac:7f:b0:c3
              ASN1 OID: brainpoolP256r1
          X509v3 extensions:
            X509v3 Basic Constraints:
              CA:FALSE
          X509v3
              Key Usage: Digital Signature
              Signature
                Algorithm: ecdsa-with-SHA256
                30:45:02:20:2b:6d:80:e3:ea:a0:c1:19:5d:69:72:e1:e6:0c:
                76:77:0f:52:4d:55:6b:6e:44:31:fc:22:4a:6e:a7:2b:5d:3a:
                02:21:00:a3:7c:75:ed:3a:61:68:0e:ef:8b:4b:6b:47:36:05:
                b5:ec:26:45:68:37:6a:ed:2b:b0:a5:ba:3e:79:db:2b:78
```

Beispiel 3.1. Gültiges Zertifikat nach den beschriebenen Anforderungen

4. Zertifikatsprofile am HAN

4.1. Einleitung

Die HAN-Zertifikate, die das SMGW für sich erstellt, verwendet und akzeptiert, verwenden die Syntax und Semantik von X.509-Zertifikaten in der Version 3 nach [RFC5280] Kapitel 4 und **SOLLEN** je nach Zertifikatstyp in ▸Tabelle 4.1 konform zu einem der in diesem Kapitel beschriebenen Zertifikatsprofiltypen sein: [REQ.ZertifikateHAN.Allgemein.10]

- Typ A: Selbstsigniert, nicht aus der SM-PKI
- Typ B: Zertifikat durch die CA des GWA oder GWH ausgestellt/signiert

ICS.ZertifikateHAN.Allgemein.10

Der Hersteller **MUSS** im ICS deklarieren, ob das SMGW die Anforderungen an die selbstsignierten (Typ A) HAN-Zertifikatsprofile für das SMGW und die HAN-Teilnehmer für die vom SMGW erzeugten und verarbeiteten HAN-Zertifikate umsetzt und die Abweichungen in einer Anlage zum ICS beschreiben.

ICS.ZertifikateHAN.Allgemein.20

Der Hersteller **MUSS** im ICS deklarieren, ob das SMGW die Anforderungen an die Typ B HAN-Zertifikatsprofile für SRV und SMGW für die vom SMGW erzeugten und verarbeiteten HAN-Zertifikate umsetzt und die Abweichungen in einer Anlage zum ICS beschreiben.

Zertifikatstyp	Zertifikats-Profiltyp	Aussteller
GW_HAN_TLS_CRT	Typ A	SMGW
SRV_HAN_TLS_CRT	Typ A	SRV
SRV_HAN_TLS_CRT	Typ B	GWACA, GWHCA
CON_HAN_TLS_CRT	Typ A	CON
CON_HAN_TLS_CRT	Typ B	GWACA, GWHCA
CLS_HAN_TLS_CRT	Typ A	CLS
GWACA_SIG_CRT	Typ A	GWACA
GWHCA_SIG_CRT	Typ A	GWHCA

Tabelle 4.1 Zertifikatsprofiltypen der HAN-Zertifikate

Die folgenden Abschnitte enthalten Tabellen in denen Anforderungen an das Vorhandensein von Attributen und Datenfeldern verschiedener Zertifikatsprofile beschrieben sind. Darin werden die folgenden Abkürzungen verwendet:

Zeichen	Langform	Bedeutung
m	Mandatory	Das Element muss vorhanden sein.
x	Not existent	Das Element darf nicht vorhanden sein.
o	Optional	Das Element kann vorhanden sein

Zeichen	Langform	Bedeutung
c	Conditional	Das Element ist abhängig von einem anderen Element vorhanden
r	Recommended	Das Element soll vorhanden sein.

Tabelle 4.2 Beschreibung der Abkürzung zum Vorhandensein von Zertifikats-Elementen

4.2. Laufzeit

Eine Prüfung der zeitlichen Gültigkeit von selbstsignierten (Typ A) Zertifikaten durch das SMGW wird nicht vorgegeben, da der GWA des SMGW verantwortlich ist, dass das SMGW nur gültigen, selbst-signierten Zertifikaten vertraut und dies über die HAN- und Proxy-Kommunikationsprofile parametriert.[1] Dennoch sollen die Verwender des GW_HAN_TLS_CRT im HAN Kenntnis über den geplanten Verwendungszeitraum der SMGW-Zertifikate erhalten können. Die Laufzeit richtet sich nach der erwarteten Sicherheit der verwendeten kryptografischen Verfahren unter Berücksichtigung einer möglichen kryptografischen Migration und entspricht der Laufzeit von Zertifikaten am LMN gemäß [TR-03109-3].

Das SMGW **MUSS** die zeitliche Gültigkeit von SRV_HAN_TLS_CRT Zertifikaten vom Typ B und von und von dessen GWACA_SIG_CRT-Zertifikaten oder GWHCA_SIG_CRT-Zertifikaten prüfen. [REQ.Zertifikate-HAN.Allgemein.20]

ICS.ZertifikateHAN.Allgemein.30

Der GWH **MUSS** im ICS deklarieren, welche Laufzeit (aufgerundet in Monaten) die vom SMGW erstellten GW_HAN_TLS_CRT-Zertifikate besitzen (0: Wenn die Laufzeit nicht begrenzt ist).

4.3. Zertifikatsstruktur

Zertifikatsfeld	Referenz in RFC5280	Element vorhanden	Wert
TBSCertificate	4.1.1.1	m	Siehe ▸Tabelle 4.4
SignatureAlgorithm	4.1.1.2	m	Siehe ▸Abschnitt 4.3.1
SignatureValue	4.1.1.3	m	Abhängig vom gewählten Signatur-Algorithmus nach [TR-03109-3]: • Typ A: Mit dem privaten Schlüssel zum "subjectPublicKeyInfo" selbstsigniert • Typ B: Mit dem privaten Schlüssel GWACA_SIG_PRV oder GWHCA_SIG_PRV signiert.

Tabelle 4.3 Struktur des Elementes "Certificate"

Die folgende Tabelle gibt die Struktur des Feldes "TBSCertificate" verbindlich vor.

Zertifikatsfeld	Referenz in RFC5280	Element vorhanden	Wert
Version	4.1.2.1	m	'v3'
SerialNumber	4.1.2.2	m	Zufällig gewählte, positive Ganzzahl, bestimmt vom Aussteller (8-20 Octets).
Signature	4.1.2.3	m	Gleicher Wert wie im Feld "SignatureAlgorithm" (s. ▸Abschnitt 4.3.1).

[1] Geräte im HAN haben nach der Inbetriebnahme zunächst oft keine zuverlässige Kenntnis über die Zeit. Eine Prüfung der zeitlichen Gültigkeit ist hier nur eingeschränkt möglich.

Zertifikatsfeld	Referenz in RFC5280	Element vorhanden	Wert
Issuer	4.1.2.4	m	Eindeutiger Name (Distinguished Name, DN) des Zertifikatsinhabers siehe ▸Abschnitt 4.3.3: • Für Typ A (selbstsignierte) HAN-Zertifikate identisch zu "Subject". • Für Typ B: *SubjectCN* der ausstellenden CA
Validity	4.1.2.5	m	Zeitpunkte für Beginn und Ende der Gültigkeit des Zertifikates (s. ▸Abschnitt 4.3.4).
Subject	4.1.2.6	m	Eindeutiger Name (Distinguished Name, DN) des Zertifikatsinhabers siehe ▸Abschnitt 4.3.3.
SubjectPublicKeyInfo	4.1.2.7	m	Siehe ▸Abschnitt 4.3.2.
IssuerUniqueId	4.1.2.8	x	Entfällt
SubjectUniqueId	4.1.2.8	x	Entfällt
Extensions	4.1.2.9	m	Siehe ▸Abschnitt 4.3.5.

Tabelle 4.4 Struktur des Elementes "TBSCertificate"

4.3.1. SignatureAlgorithm

Durch die Datenstruktur SignatureAlgorithm wird nach [RFC5280] der Signaturalgorithmus des Zertifikats angegeben. Dieser besteht aus der folgenden Datenstruktur:

```
AlgorithmIdentifier ::= SEQUENCE {algorithm OBJECT IDENTIFIER, parameters ANY DEFINED BY algorithm OPTIONAL}
```

Der Wert von "algorithm" muss nach den Vorgaben zur TLS-Kommunikation im HAN nach [TR-03109-3] gewählt werden. Das Datenfeld "parameters" muss leer bleiben.

4.3.2. SubjectPublicKeyInfo

Das Feld "SubjectPublicKeyInfo" besitzt folgende Struktur (s. [RFC5480]):

```
SubjectPublicKeyInfo ::= SEQUENCE {algorithm AlgorithmIdentifier, subjectPublicKey BIT STRING}
```

Die OID im Datenfeld "algorithm" enthält den Wert 1.2.840.10045.2.1 (id-ecPublicKey). Im Feld "ECParameters" ist gemäß [RFC5480] die Variante namedCurve zu verwenden. Für die aktuell zu verwendenden Werte siehe [TR-03109-3] TLS-Kommunikation im HAN.

Der PublicKey wird mit unkomprimierten Punktkoordinaten angegeben.

4.3.3. Issuer und Subject

- Das Namensschema für den "commonName" der HAN-Teilnehmer lehnt sich an [SM-PKI-CP] Anhang A an.
- Für Typ A (selbstsignierte) HAN-Zertifikate müssen "subject" und "issuer" gemäß [RFC5280] identisch sein.
- Einzelne Attribute von Issuer und Subject dürfen nicht länger als 64 Zeichen sein.
- Vorgaben an das Namensschema von Issuer und Subject sind in ▸Abschnitt 4.4 und ▸Abschnitt 4.5 beschrieben.

4.3.4. Validity

- Das Feld "notBefore" enthält den Erzeugungszeitpunkt des Schlüsselpaares und des Zertifikates.

- Das Feld "notAfter" enthält den Zeitpunkt, nach dem das Zertifikat und das dazugehörige Schlüsselpaar nicht mehr verwendet werden darf. Der Zeitpunkt muss nach dem Erzeugungszeitpunkt liegen.

4.3.5. Extensions

Die nun folgende Tabelle enthält eine Übersicht der Extensions und den Anforderungen an deren Vorhandensein.

Bezeichnung	Typ A: Vom HAN-Teilnehmer Selbstsigniert	Typ B: Ausgestellt durch CA (nicht SM-PKI)
AuthorityKeyIdentifier	o	m
SubjectKeyIdentifier	o	m
KeyUsage	r	r
PrivateKeyUsagePeriod	x	x
CertificatePolicies	x	o
SubjectAltNames	c (Bisher m)	o
BasicConstraints	r cA=FALSE	m cA=FALSE
ExtendedKeyUsage	r	r
CRLDistributionPoints	x	o
Weitere Extensions	o	x

Tabelle 4.5 Extensions

4.3.5.1. KeyUsage

- Extension-ID (OID): 2.5.29.15
- Kritisch: Nein
- Beschreibung: Die Extension KeyUsage (spezifiziert in [RFC5280], 4.2.1.1) definiert, für welche Zwecke der zertifizierte öffentliche Schlüssel verwendet werden darf.
- Gesetzte Bits: digitalSignature(0)[2].

4.3.5.2. BasicConstraints

- Extension-ID (OID): 2.5.29.19
- Kritisch: Ja für Typ B Zertifikate, Nein für Typ A Zertifikate
- Beschreibung: Diese Extension (spezifiziert in [RFC5280], 4.2.1.9) gibt an, ob es sich bei dem gegebenen Zertifikat um eine CA handelt und wie viele CAs ihr folgen können.

4.3.5.3. SubjectAltName

- Extension-ID (OID): 2.5.29.27
- Kritisch: Ja
- Beschreibung: Diese Extension (spezifiziert in [RFC5280], 4.2.1.6) ermöglicht die Bindung von Identitäten an das Subject des Zertifikates. Diese Angabe ist alternativ oder zusätzlich zur Identifikation im Subject möglich.
- "dNSName": Es wird empfohlen, die eindeutige Kennung von SMGW oder HAN-Teilnehmer basierend auf [DIN43863-5] mit angehängtem ".sm" oder eine auf der Komponente des HAN-Teilnehmers lesbare, prak-

[2] Für CLS-TLS-Zertifikate sind weitere Key Usages zulässig

tisch eindeutige, nicht-wechselnde, herstellerübergreifende Netzwerkschnittstellenadresse (MAC/EUI) mit angehängtem ".eui" als Domain Name Label zu verwenden.

4.3.5.4. ExtendedKeyUsage

- Extension-ID (OID): 2.5.29.37
- Kritisch: Nein
- Beschreibung: Die Extension ExtendedKeyUsage (spezifiziert in [RFC5280], 4.2.1.12) gibt an, ob das Zertifikat als TLS-Client und/oder als TLS-Server-Zertifikat genutzt werden kann.
- Die HAN-Teilnehmer Zertifikate sollen sowohl für TLS-Web-ServerAuthentifikation (1.3.6.1.5.5.7.3.1) als auch für TLS-Web-ClientAuthentifikation (1.3.6.1.5.5.7.3.2) verwendet werden.

4.4. Anforderungen an die HAN-TLS-Zertifikate des SMGW

4.4.1. Einleitung

Zusätzlich zu den Anforderungen an Typ A HAN-Zertifikate nach ▸Abschnitt 4.3 gelten für *GW_HAN_TLS_CRT*-Zertifikate die Anforderungen in ▸Abschnitt 4.4.

4.4.2. Namensschema der SMGW-HAN-Zertifikate

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	r	"<id>.sm"	<id> Herstellerübergreifende Identifikationsnummer für Messeinrichtungen nach [DIN43863-5] mit der Sparte "E".
organisation	O	o	"<O>"	Falls verwendet darf das Feld "SM-*PKI" nicht enthalten.
organisational unit	OU	o	"<GWA-ID>"	Name des für das SMGW zuständigen GWA (aus "common name" des *GWA_WAN_SIG_CRT*).
country	C	r	"<LC>"	Zwei Zeichen Ländercode gemäß [ISO 3116 ALPHA-2]
serial number	SERIAL NUMBER	r	"<SN>"	Sequenznummer der Zertifikats im Bereich von 1 bis 2^31-1 und startet bei 1. Diese wird bei jedem neuen Zertifikat um den Wert 1 hochgezählt.

Tabelle 4.6 Namensschema der SMGW-HAN-Zertifikate

4.5. Anforderungen an die TLS-Zertifikate der HAN-Teilnehmer

4.5.1. Einleitung

Zusätzlich zu den Anforderungen an Typ A oder Typ B HAN-Zertifikate nach ▸Abschnitt 4.3 gelten für *CON_HAN_TLS_CRT*, *SRV_HAN_TLS_CRT* und *CLS_HAN_TLS_CRT*-Zertifikate die Anforderungen in ▸Abschnitt 4.5.

4.5.2. Namensschema der HAN-Teilnehmer-Zertifikate

HAN-Teilnehmerzertifikate (außer *GW_HAN_TLS_CRT*) enthalten folgende Distinguished Name Attribute:

Attribut Typ	Kürzel	Vorgabe	Wert	Erläuterung
common name	CN	r	"<id>[.<idschema>]"	• Sofern <idschema> gleich "sm" ist, enthält <id> die auf der HAN-Komponente ablesbare, 14-stellige herstellerübergreifende Identifikationsnummer für Messeinrichtungen nach [DIN43863-5] • Sofern <idschema> gleich "eui" ist, enthält <id> die auf der HAN-Komponente ablesbare praktisch eindeutige, nicht-wechselnde, herstellerübergreifende Netzwerkschnittstellenadresse (MAC/EUI) • Die <id> und das <idschema> für Service-Techniker und Letztverbraucher-Zertifikate wird gemäß organisatorischer Anforderungen des Ausstellers vergeben und vom GWA im SMGW konfiguriert.
country	C	o	"<LC>"	Zwei Zeichen Ländercode gemäß [ISO 3116 ALPHA-2]
serial number	SERIAL NUMBER	o	"<SN>"	Falls vorhanden, enthält das Feld die Sequenznummer des Zertifikats im Bereich von 1 bis 2^31-1. und startet bei 1. Diese wird bei jedem neuen Zertifikat um den Wert 1 hochgezählt.

Tabelle 4.7 Namensschema der HAN-Teilnehmer-Zertifikate

Der Distinguished Name darf weitere Attribute enthalten (nicht empfohlen). Eine Prüfung durch das SMGW erfolgt aktuell nicht.

4.6. Anforderungen an das CA-Zertifikat zur Validierung der Zertifikate der Servicetechniker

4.6.1. Einleitung

Zusätzlich zu den Anforderungen an selbstsignierte (Typ A) HAN-Zertifikate nach ▸Abschnitt 4.3 gelten für *GWACA_SIG_CRT*- und *GWHCA_SIG_CRT*-Zertifikate die Anforderungen in ▸Abschnitt 4.6

4.6.2. Namensschema des CA-Zertifikates des GWA/GWH zur Validierung der Zertifikate der Servicetechniker

Es wird empfohlen, die Attribute des Distinguished Name (Subject/Issuer) in Anlehnung an [SM-PKI-CP] Anhang A zu wählen.

5. CMS

5.1. Einleitung

Dieses Kapitel beschreibt Anforderungen an die Inhaltsdatenverschlüsselung und -signatur unter Verwendung von CMS. Es enthält Anforderungen an die Kommunikation zwischen einem Sender (Originator) und dem zugehörigen Empfänger (Recipient) und konkretisiert die Anforderungen allgemeiner CMS-Spezifikationen zur Verwendung in intelligenten Messsystemen.

Die Beschreibung der Anforderungen an die Konfiguration der Parameter, Zertifikate und die Zertifikatsvalidierung für CMS sind nicht Bestandteil dieses Kapitels.

5.2. Anforderungen

- Die Implementierung **MUSS** die Datenstrukturen ContentInfo, SignedData, AuthEnvelopedData nach [TR-03109-1-I] verarbeiten und erzeugen. [REQ.CMS.Implementierung.10]
- Die Implementierung **SOLL** die Datenstrukturen CompressedData nach [RFC3274] und ZLIB mit deflate-Codierung nach [RFC1951] und [RFC1950] verarbeiten und erzeugen. [REQ.CMS.Implementierung.20]
- Die Implementierung **MUSS** Zertifikate nach [RFC5280] Kapitel 4.1 verarbeiten und validieren. [REQ.CMS.Implementierung.30]
- Die Implementierung **MUSS** die MessageCipherSuite (s. ▸Tabelle 5.1) CMSSuiteA1, CMSSuiteA2, CMSSuiteA3, CMSSuiteA4 verarbeiten und erzeugen. [REQ.CMS.Implementierung.40]

5.2.1. MessageCipherSuite

Suite	Key Agreement Algorithm, KDF und KDF-Hash	Key Encryption Algorithm	Authentication und Content Encryption Algorithm	Compression Algorithm
CMSSuiteA1	ecka-eg-X693K-DF-SHA256 (Definiert in [TR-03111])	id-aes128-wrap (Definiert in [RFC3565])	id-aes128-GCM (Definiert in [RFC5084])	id-alg-zlibCompression (Definiert in [RFC3274])
CMSSuiteA2	ecka-eg-X693K-DF-SHA256 (Definiert in [TR-03111])	id-aes128-wrap (Definiert in [RFC3565])	id-aes-CBC-CMAC-128 (Definiert in [TR-03109-1-I] Anhang A)	id-alg-zlibCompression (Definiert in [RFC3274])
CMSSuiteA3	ecka-eg-X693K-DF-SHA256 (Definiert in [TR-03111])	id-aes128-wrap (Definiert in [RFC3565])	id-aes128-GCM (Definiert in [RFC5084])	Keine CMS-Datenkompression
CMSSuiteA4	ecka-eg-X693K-DF-SHA256 (Definiert in [TR-03111])	id-aes128-wrap (Definiert in [RFC3565])	id-aes-CBC-CMAC-128 (Definiert in [TR-03109-1-I] Anhang A)	Keine CMS-Datenkompression

Tabelle 5.1 MessageCipherSuites

Im Rahmen einer künftigen kryptografischen Migration ist geplant, die nächste Suite CMSSuiteB zu benennen.

6. RESTful Webservice

6.1. Einleitung

Das Hypertext Transfer Protokoll (HTTP) ist ein OSI Layer 7 Protokoll, das zwischen Transaktionen zustandslos ist. Es ermöglicht die Zusammenarbeit von Informationssystemen über ausgetauschte Textnachrichten (HTTP-Request und HTTP-Response genannt). Das Protokoll definiert dabei das Interface, um mit den Ressourcen zu interagieren.

Die RFCs [RFC7230], [RFC7231] und [RFC7233] bilden den Rahmen der Anforderungen an die Implementierung. Sie beschreiben aber auch viele Protokoll-Optionen. Für den interoperablen Betrieb und da die Implementierung über begrenzte Ressourcen verfügt, sind die Optionen allerdings nicht vollumfänglich zu implementieren. Insbesondere Aspekte wie Datenvolumen und Migration zwischen Versionen begründen eine Einschränkung auf die notwendigen Protokoll-Optionen für einen leistungsfähigen und interoperablen Betrieb.

Die umgesetzten Optionen des HTTP-Servers und HTTP-Clients der Implementierung sollen den Vorgaben der [RFC7230] und [RFC7231] entsprechen

6.2. Anforderungen

▸Abschnitt 6.2 nennt Anforderungen an die Implementierung, die immer dann beachtet werden müssen, wenn HTTP an den von außen zugänglichen Schnittstellen eingesetzt wird.

REQ.Webservice.Http.10

Die Implementierung **MUSS** das Format, d.h. die Syntax, der HTTP-Nachrichten an den von außen zugänglichen Schnittstellen gemäß der Spezifikation in [RFC7230] Kapitel 3 verarbeiten und senden.

REQ.Webservice.Http.20

Die Implementierung **MUSS** jede von außen zugängliche Ressource (Firmware-Dateien, Konfigurationsobjekte, Statusinformationen, NTP-Daten etc.) durch einen Uniform Resource Identifier (URI) nach [RFC3986] identifizieren.

REQ.Webservice.Http.30

Die Implementierung **MUSS** die Bezeichner der HTTP-Header-Fields case-insensitiv verarbeiten.

REQ.Webservice.HttpClient.50

Die Implementierung **MUSS** HTTP-Statuscodes gemäß [RFC7231] verarbeiten können.

REQ.Webservice.Http.60

Die Implementierung **MUSS** sicherstellen, dass HTTP-Header-Fields in Request und Response eindeutig sind. Die Implementierung **DARF NICHT** Bezeichner von HTTP-Header-Fields mehrfach verwenden bzw. akzeptieren. Ausnahme davon sind die HTTP-Header-Fields "Accept", "Link" und "WWW-Authenticate".

REQ.Webservice.Http.80

Die Implementierung **MUSS** sicherstellen, dass die HTTP-Request-Response-Transaktion in der Implementierung beendet wird, wenn die TLS-Verbindung getrennt wird.

REQ.Webservice.HttpServer.90

Die Implementierung **MUSS** HTTP Status Codes 200-204 senden, wenn eine Anfrage an den Server ohne Fehler beendet wurde und Status Codes größer oder gleich 400 verwenden, wenn eine Anfrage mit Fehler beendet wird.

REQ.Webservice.HttpServer.100

Die Implementierung **MUSS** die Methoden GET, PUT, POST, DELETE mit der Semantik gemäß [RFC7231] verarbeiten.

6.3. URI Query-Parameter

6.3.1. Einleitung

QueryParameter können Bestandteil einer URI nach [RFC3986] sein. Diese werden zur Selektion von Ressourcen in RESTful APIs verwendet. Da die Syntax des Query Strings "query" nicht in [RFC3986] Kapitel 3.4 beschrieben ist, spezifiziert diese Detailspezifikation die Struktur und Syntax der Query Parameter.

6.3.2. Struktur und Syntax der URI QueryParameter

Die Grammatik der *QueryParameter* wird mit Augmented BNF nach [RFC5234] beschrieben:

Der Query String wird durch ein "?" eingeleitet. Auf dieses Zeichen folgen die *QueryParameter*. Die *QueryParameter* **SOLLEN** nach der Bildungsregel <query-component> validiert werden. [REQ.HTTP.QueryParameter.10]

query-component = parameter [*("&" parameter)]

parameter = name "=" value

name = *qchar mit einer Länge von 1..50 Zeichen

value = *qchar mit einer Länge von 0..255 Zeichen

qchar = unreserved / pct-encoded / qspecial

qspecial = "/" / "?" / ":" / "@" / "!" / "$" / "'" / "(" / ")" / "*" / "+" / "," / ";"

Die folgenden Regeln sind in [RFC3986] (normativ) definiert. Sie werden hier wiederholt:

unreserved = ALPHA / DIGIT / "-" / "." / "_" / "~"

pct-encoded = "%" HEXDIG HEXDIG

Anmerkung

- Diese Grammatik erlaubt die Verwendung aller nach [RFC3986] zulässigen Zeichen.
- In der URI ist kein Leerzeichen erlaubt (s. [RFC3986] Appendix C).
- [RFC3986] erlaubt keine leeren QueryParameter. D.h. falls "?" in der URI vorkommt, dann muss mindestens ein Parameter folgen.
- Die oben definierte Regel <qchar> entspricht der Regel <pchar> aus [RFC3986], die die zulässigen Zeichen für die *QueryParameter* definiert, ohne die Zeichen "=" und "&".

7. Authentifizierung mittels Kennung und Passwort

7.1. Einleitung

Dieses Kapitel beschreibt die Anforderungen an die Authentifizierung von Nutzern über die HAN Schnittstelle des SMGW mittels Kennung und Passwort.

Die Authentifizierung erfolgt über das HTTP-Digest Authentifizierungsverfahren. Dabei sendet der Nutzer zunächst einen HTTP-Request an das SMGW, um auf eine Ressource über eine URI zuzugreifen. Das SMGW berechnet eine zufällige "Challenge" und den "Realm" (Bereich), für den die Authentifizierung erforderlich ist. Der Nutzer wird aufgefordert seine Kennung und sein Passwort im Web-Client des Nutzers einzugeben. Aus der Challenge, einer Nonce, der URI und dem Hash über Realm, Kennung und Passwort berechnen sowohl SMGW als auch Web-Client einen Hash ("Digest"). Der Web-Client sendet den Hash an das SMGW. Nur falls der vom SMGW berechnete Hash mit dem vom Web-Client empfangenen Hash übereinstimmt, wird die Autorisierung zum Zugriff auf die Ressource (URI) erteilt.

7.2. Anforderungen

Das SMGW **MUSS** die Authentifizierung über HTTP-Digest Authentication gemäß [RFC7616] durchführen. [REQ.BenutzerAuth.Allgemein10]

Das SMGW **SOLL** die Digest-Berechnung basierend auf dem SHA-256 Verfahren anbieten. [REQ.BenutzerAuth.Allgemein20]

Das SMGW **KANN** die Digest-Berechnung basierend auf dem MD5 Verfahren anbieten. [REQ.BenutzerAuth.Allgemein30]

ICS.BenutzerAuth.Allgemein10

Der GWH **MUSS** im ICS deklarieren, ob das SMGW für die Digest-Authentifizierung nach [RFC7616] das SHA-256-Verfahren unterstützt.

ICS.BenutzerAuth.Allgemein20

Der GWH **MUSS** im ICS deklarieren, ob das SMGW das MD5-Verfahren unterstützt.

8. Bidirektionale LMN-Kommunikation über HDLC

8.1. Einleitung

Diese Detailspezifikation konkretisiert die Anforderungen an das SMGW als TLS-Client und HDLC-Primary-Station zur bidirektionalen LMN-Kommunikation über eine physische RS-485-Schnittstelle.

8.2. Anforderungen

- Das SMGW **MUSS** die leitungsgebundene, asynchrone, serielle, Halb-Duplex-Kommunikation nach EIA/RS-485 zwischen Messeinrichtung und SMGW gemäß [DIN VDE 0418-63-7] umsetzen. [REQ.TLSHDLC.Bidirektional.10]
- Das SMGW **MUSS** das HDLC Link-Layer- und Transportprotokoll nach den Anforderungen der Spezifikation [ISO13239] als primäre Kommunikationsstation gemäß der Anforderungen nach [DIN VDE 0418-63-7] umsetzen, um eine zuverlässige Übertragung zu gewährleisten. [REQ.TLSHDLC.Bidirektional.20] Das SMGW **MUSS** die automatische Zuordnung (Adressauflösung) von HDLC Adressen und Identifikation der Messeinrichtung nach [DIN43863-5] gemäß [DIN VDE 0418-63-7] umsetzen. [REQ.TLSHDLC.Bidirektional.30]
- Das SMGW **MUSS** TLS nach den Anforderungen von [TR-03109-3] in der Rolle des TLS-Clients gemäß der Anforderungen nach [DIN VDE 0418-63-7] umsetzen, um vertrauliche und authentische Transportverbindungen zwischen SMGW und einem Kommunikationspartner zu gewährleisten. [REQ.TLSHDLC.Bidirektional.40]
- Das SMGW **MUSS** die initiale kommunikative Anbindung der Messeinrichtung an das SMGW mit dem Symmetrischen Verfahren nach [TR-03109-3] gemäß [DIN VDE 0418-63-7] mit geräteindividuellen "Master-Key" MK0 der Messeinrichtung umsetzen, um authentisch Zertifikate auszutauschen und das vom SMGW erzeugte Schlüsselpaar der Messeinrichtung vertraulich an die Messeinrichtung zu übermitteln. [REQ.TLSHDLC.Bidirektional.50]

9. Detailspezifikation Wireless MBUS

9.1. Einleitung

Das Wireless M-Bus-Protokoll beschreibt Kommunikationsverfahren von energie- und speicherbegrenzten Messeinrichtungen mit einem Gateway über eine Funk-Kommunikationsstrecke mit geringer Bandbreite. Die Rollen der Kommunikationspartner werden in der englischen Literatur mit "Meter" und "Other" bzw. "Gateway" bezeichnet.

Dieses Kapitel beschreibt die Anforderungen an die Implementierung der Protokolle und Nachrichtenformate eines unidirektionalen Empfängers. Es enthält Anforderungen an die Kommunikation zwischen den Kommunikationspartnern "Meter" und "Gateway" und konkretisiert die Anforderungen der DIN EN 13757-Spezifikationen zur Verwendung in intelligenten Messsystemen.

Die Messwerte werden in Nachrichten der Anwendungsschicht übertragen. Diese Nachrichten bestehen aus Datagrammen der Verbindungsschicht. Sofern eine Nachricht zu groß ist, um in einem Datagram übertragen zu werden, wird sie beim Absender fragmentiert und beim Empfänger reassembliert.

Ein oder mehrere Messwerte werden in Datensätzen aus Datentyp (Dateninformationsblock, DIB), Messwertidentifikation, Einheit, Skalierungsfaktor (Wertinformationsblock, VIB) und Wert im M-Bus Applikationsformat übermittelt.

Der Absender verschlüsselt jede Nachricht authentisch mit einem gemeinsamen nachrichten- und messeinrichtungsindividuellen, symmetrischen Schlüssel. Der Empfänger prüft die Authentizität der Nachricht und entschlüsselt diese mit dem gemeinsamen Schlüssel.

Die Messgrößen und Messarten der in den Datensätzen codierten Messwerte werden zur Weiterverarbeitung im SMGW über OBIS-Kennzahlen identifiziert.

Folgende Kapitel der [EN13757-3] sind für die Interoperabilität relevant:

- Kapitel 5.2 (M-Bus Protokoll) mit den Einschränkungen dieser Detailspezifikation.
- Anhang E.1 (Fehler-Flag).
- Anhang F (Profile). Compact Profile für Messwertbündel. Die zur Abrechnung verwendeten Zeitstempel der Messwerte müssen im Gateway gebildet werden.
- Anhang H.2 (Abbildung auf OBIS-Kennzahlen), ergänzt um [OMSS4] Annex A.

Folgende Anforderungen der [EN13757-3] werden nicht gefordert:

- Kapitel 5.3 (Application Selection) ist für unidirektional kommunizierende Messeinrichtungen nicht umsetzbar.
- Kapitel 5.4 (Clock Synchronisation) ist für unidirektional kommunizierende Messeinrichtungen nicht umsetzbar.
- Kapitel 5.5/Anhang D (Alarm Status) wird nicht für die Interoperabilität gefordert, da der Status über das Datenfeld "STS" des TPL-Header übermittelt wird.
- Kapitel 5.6.2 (Application Error Protocol) ist für unidirektional kommunizierende Messeinrichtungen nicht umsetzbar.
- Kapitel 5.7 (Baudrate Selection) ist für Wireless M-Bus Messeinrichtungen nicht umsetzbar.

- Kapitel 5.8 (Aktion synchronisieren) ist für unidirektional kommunizierende Messeinrichtungen nicht umsetzbar.
- Kapitel 5.9 (Herstellerspezifische Anwendungsprotokolle) werden nicht verarbeitet.
- Kapitel 5.10 (Andere Anwendungsprotokolle) werden nicht verarbeitet.
- Kapitel 5.10 (Image-Übertragung) ist für unidirektional kommunizierende Messeinrichtungen nicht umsetzbar.
- Anhang C (VIF-Codierung für Sondereinheiten) wird nicht gefordert, bzw. ist für unidirektional kommunizierende Messeinrichtungen nicht umsetzbar.
- Anhang E.2 (Übergabe der Fernsteuerung) ist für unidirektional kommunizierende Messeinrichtungen nicht umsetzbar.
- Anhang E.3 (Uhrensynchronisation) ist für unidirektional kommunizierende Messeinrichtungen nicht umsetzbar.
- Anhang G (Kompakter Rahmen)
- Anhang H.3 (Online Ergänzung eines OBIS-Eintrages).
- Anhang I (Image Transfer) ist für unidirektional kommunizierende Messeinrichtungen nicht umsetzbar.

9.2. Anforderungen

- Das SMGW **MUSS** die physische Medienzugangsschicht für drahtlose Kommunikation nach [EN13757-4] als Short Range Device Funkempfänger mit Mode T umsetzen. [REQ.WMBUS.Unidirektional.30]
- Das SMGW **SOLL** die physische Medienzugangsschicht für drahtlose Kommunikation nach [EN13757-4] mit Mode C mit Rahmenformat A als Funkempfänger unterstützen. [REQ.WMBUS.Unidirektional.36] [1] (s. ▸ICS.WMBUS.wmbus.30)
- Das SMGW **MUSS** den Data Link Layer und Extended Link Layer nach den Anforderungen der Spezifikation nach [EN13757-4] und nach [OMSS4] Abschnitte 5.2 und 5.3 in der Rolle des Gateway umsetzen, um den Transport der Nachrichten und die Integrität der Verbindungen zu gewährleisten. [REQ.WMBUS.Unidirektional.40]
- Das SMGW **MUSS** die Authentifizierung und Entschlüsselung von Nachrichten (AFL) nach den Anforderungen der Spezifikation [EN13757-7] Security Mode 7 für das SMGW in der Rolle des Recipients ("Gateway") umsetzen ([OMSS4] Security Profile "B"). [REQ.WMBUS.Unidirektional.50]
- Das SMGW **SOLL** die Anforderungen nach [OMSS4] Annex E.1.1.1 für unidirektional kommunizierende Zähler zur Verbesserung der Interoperabilität unterstützen. [REQ.WMBUS.Unidirektional.70]
- Das SMGW **SOLL** für den Empfang von Messwertbündeln das "Compact Profile" nach [EN13757-3] Anhang F nach den Anforderungen der [OMS-TR-07] Kap. 6 umsetzen. [REQ.WMBUS.apl.10] (s. ▸ICS.WMBUS.wmbus.10)
- Das SMGW **MUSS** die empfangene Anwendungsnachricht gemäß [EN13757-3] Kapitel 5.2 interpretieren. [REQ.WMBUS.apl.20]
- Falls dem M-Bus-Datenblock herstellerspezifische Daten folgen, **DARF** die Implementierung diese Daten **NICHT** für die Messwertverarbeitung heranziehen. [REQ.WMBUS.apl.30]

[1] In künftigen Versionen der Technischen Richtlinie muss Mode C implementiert werden.

9.3. ICS

ICS.WMBUS.wmbus.10

Der GWH **MUSS** im ICS deklarieren, ob das SMGW den Empfang von Messwertbündeln nach ▸REQ.WMBUS.apl.10 unterstützt.

ICS.WMBUS.wmbus.30

Der GWH **MUSS** im ICS deklarieren, ob das SMGW den Empfang von wM-BUS Nachrichten nach [EN13757-4] Mode C mit Rahmenformat A unterstützt.

ICS.WMBUS.wmbus.50

Der GWH **MUSS** im ICS deklarieren, ob das SMGW die Anforderungen des [OMSS4] Annex E.1.1.1 unterstützt und in einer Anlage zum ICS die Abweichungen zu den Anforderungen beschreiben.

10. Proxy-Signalisierung mit SOCKS

10.1. Einleitung

Diese Detailspezifikation beschreibt die Verwendung von SOCKSv5 und TLS als Steuerungsprotokoll zum Verbindungsaufbau eines TLS-Proxy-Kanals vom CLS zum SMGW, um dem SMGW zu signalisieren, zu welchem aktivem EMT das SMGW eine TLS-Verbindung aufbauen soll.

10.2. Anforderungen

Sofern die Implementierung die Signalisierung des Verbindungsaufbaus vom CLS zum SMGW mittels SOCKS-Protokoll unterstützt (siehe ICS.HAN.HKS3.10 in [TRv1.1]), **MUSS** für die Initiierung und den Abbau des transparenten Kanals SOCKSv5 gemäß [RFC1928] und „TLS for SOCKSv5“ [DRAFT-IETF-AFT-SOCKS-SSL-00] verwendet werden. [REQ.SOCKS.Implementierung.10]

10.3. Ablauf

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

CLS/EMT Adressierung

Beim Verbindungsaufbau muss der Initiator (das CLS) dem SMGW mitteilen, zu welchem Endpunkt dieser eine Verbindung aufnehmen möchte.

Folgende Grafik zeigt den allgemeinen Protokollablauf bei SOCKSv5.

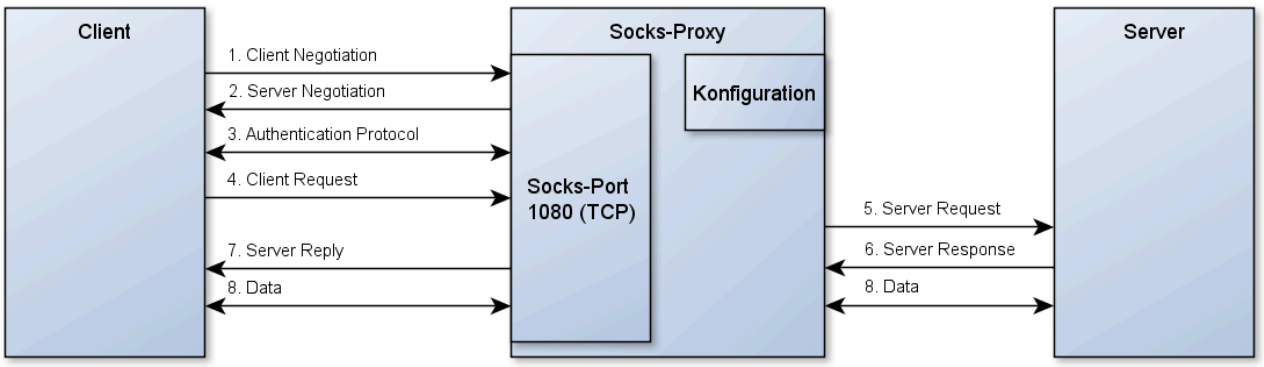

Abbildung 10.1. Protokollablauf SOCKSv5

Im SOCKSv5-ClientRequest wird zur Adressierung des aktiven EMT das Command „CONNECT“ mit einem Adresstype DomainName verwendet, welches einen Bezeichner enthält, der das aktiven EMT als Endpunkt enthält. Dieser DomainName Bezeichner ist im Proxy-Kommunikationsprofil für den Verbindungsaufbau zum aktiven EMT im SMGW eindeutig identifiziert.

Im Folgenden werden die notwendigen Prozessschritte genauer betrachtet.

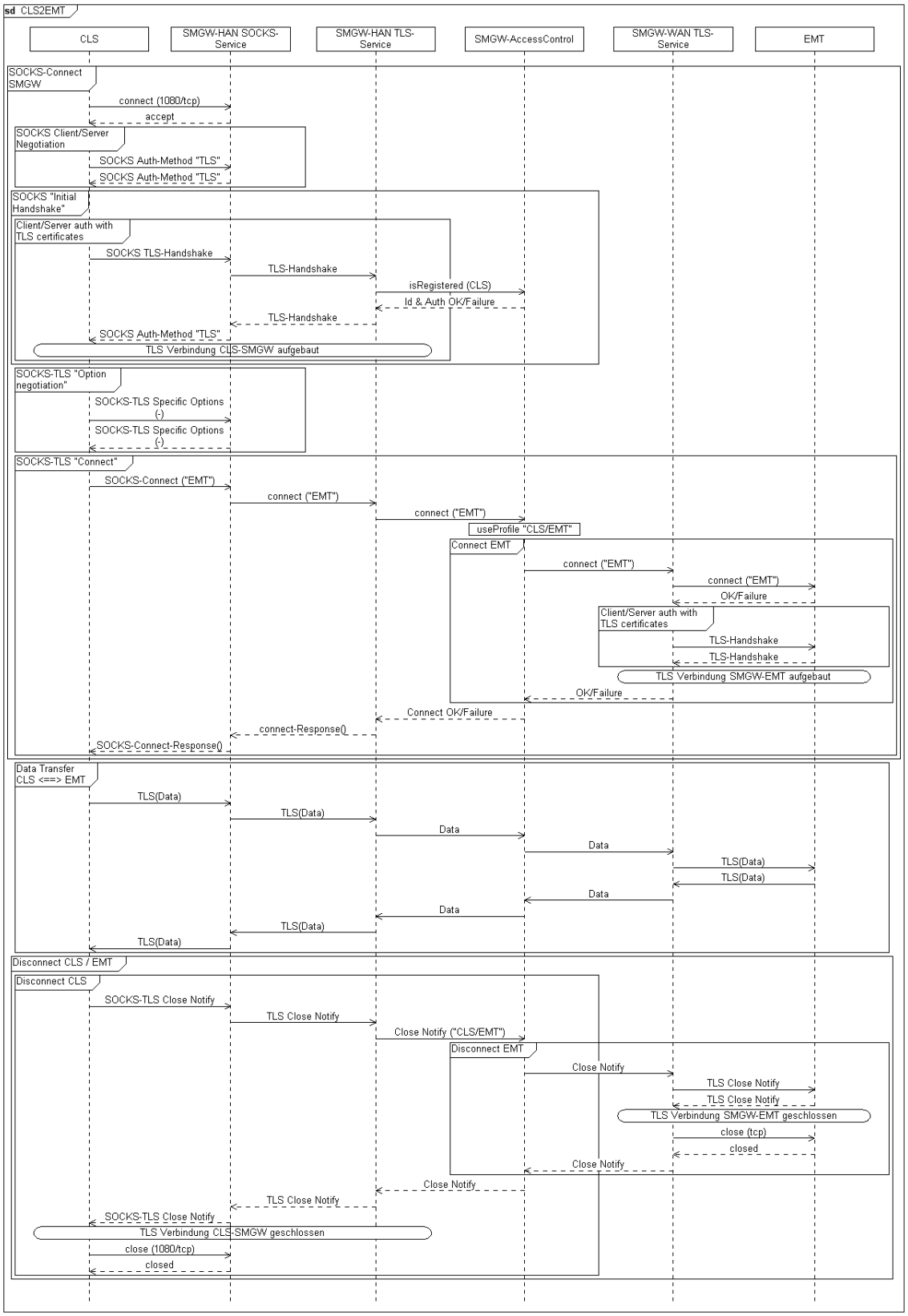

Abbildung 10.2. Sequenzdiagramm transparenter Kanal initiiert durch CLS

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

b. Vom CLS wird dabei die Authentication Method TLS[1] vorgeschlagen („Client Negotiation“).

c. Vom SOCKS-Server wird nur die „Method“ TLS akzeptiert (sonst Fehlermeldung) („Server Negotiation“).

d. Nächster Schritt ist die „Authentication“ mittels der methodenspezifischen Sub-Negotiation zwischen SOCKS Client und Server [DRAFT-IETF-AFT-SOCKS-SSL-00].

   i. Aufbau der HAN-TLS Verbindung von CLS zum SMGW (SOCKS-TLS „Initial handshake“ und „Option negotiation“).

   ii. TLS-Client-Server Identifikation und Authentifizierung mit Hilfe der Zertifikate von CLS und SMGW.

   iii. Der etablierte TLS-Kanal wird für alle weiteren SOCKS-Nachrichten der Session verwendet (SOCKS-TLS „Data-Flow“).

e. Das CLS meldet per SOCKS-Connect die gewünschte Zieladresse des aktiven EMT. („Client Request“)

f. Im Proxy-Kommunikationsprofil ist EMT als zulässiger Kommunikationspartner für das CLS festgelegt

   i. Aufbau der WAN-TLS-Verbindung von SMGW zum aktiven EMT („Server Request/Response“).

   ii. TLS-Client-Server Identifikation und Authentifizierung mit Hilfe der Zertifikate von SMGW und aktivem EMT.

   iii. SOCKS-Connect-Response an CLS („Client Response“).

g. Transparente Datenkommunikation über die beiden etablierten TLS-Tunnel.

h. Beenden der Verbindung.

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

11. Proxy-Signalisierung mit TLS Servername-Indication

11.1. Einleitung

Diese Detailspezifikation beschreibt die Verwendung der TLS-Servername Indication als Steuerungsprotokoll zum Verbindungsaufbau eines TLS-Proxy-Kanals vom CLS zum SMGW, um dem SMGW zu signalisieren, zu welchem aktivem EMT das SMGW eine TLS-Verbindung aufbauen soll.

11.2. Anforderungen

Sofern die Implementierung für die Signalisierung des zu verwendenden Proxy-Kommunikationsprofiles vom CLS zum SMGW das TLS-Protokoll einsetzt (siehe ICS.HAN.HKS3.20 in [TRv1.1]), **MUSS** das SMGW für die Initiierung des transparenten Kanals die Servername-Indication gemäß [RFC6066] unterstützen. [REQ.T-LSSNI.Implementierung.10]

11.3. Ablauf

Beim Aufbau der TLS-Verbindung zwischen CLS und SMGW wird im TLS-Handshake mittels der Zertifikate GW_HAN_TLS_CRT und CLS_HAN_TLS_CRT und der zugehörigen Schlüssel eine Client-Server Authentifizierung durchgeführt. Das CLS-Zertifikat CLS_HAN_TLS_CRT ist dabei eindeutig einem dem SMGW bekannten CLS zugeordnet. Das SMGW überprüft mittels der konfigurierten Proxy-Kommunikationsprofile die Zulässigkeit der Proxy-Verbindung und baut eine TLS-Verbindung zum konfigurierten aktiven EMT auf. Dabei wird eine TLS-Client-Server Authentifizierung zwischen SMGW und dem aktivem EMT mittels der Zertifikate GW_WAN_TLS_CRT und EMT_WAN_TLS_CRT aus der SM-PKI durchgeführt.

Der Verbindungsabbau im HAN wird über TLS-CloseNotify durch das CLS oder durch das SMGW ausgelöst.

Das SMGW beendet die HAN-TLS-Verbindung, wenn die WAN-TLS-Verbindung beendet wurde.

Das SMGW protokolliert das Ergebnis des Verbindungsaufbauversuches und Kommunikationsfehler während der Verbindung im System-Log.

CLS/EMT Adressierung

Beim Verbindungsaufbau muss der Initiator (das CLS) dem SMGW mitteilen, zu welchem Endpunkt dieser eine Verbindung aufnehmen möchte. Im Namensfeld der ClientHello-Extension "server_name" wird ein Bezeichner übermittelt, mit dem das SMGW eindeutig das Proxy-Kommunikationsprofil für den Verbindungsaufbau zum aktiven EMT bestimmen kann. Die Zeichen sind als DNS-Name gemäß RFC1035 auf a-z, Bindestrich, Punkt und 0-9 beschränkt und dürfen nicht leer sein. Der server_name soll nicht länger als 63 Zeichen sein.

12. Detailspezifikation Automatische Adresskonfiguration und DNS-Discovery

12.1. Einleitung

Dieses Kapitel beschreibt Anforderungen an die automatische, dynamische Adresskonfiguration, Device- und Service Discovery mit dem Multicast Domain Name Service Protokoll (mDNS) und Domain Name Service Service Discovery (SD) Protokoll. Multicast DNS und DNS-SD werden verwendet, um eine automatische Konfiguration von Geräten und Diensten in einem Netzwerk zu ermöglichen. Zusammen mit einer automatischen IP-Adressvergabe wird dieses Konzept "Zeroconf" genannt. Diese Spezifikation enthält Anforderungen an die Implementierung des mDNS/DNS-SD Responders (s. [RFC6762] Kapitel 6 und [RFC6763]).

Der mDNS Responder beantwortet DNS-Adressanfragen nach <SMGW-ID>.local." (unique resource) und "smgw.local." (shared resource) mit der link-lokalen Netzwerkadresse des SMGW.

mDNS verwendet die Datenstrukturen des DNS-Protokolls und kommuniziert über Port 5353 mittels UDP-Protokoll und Multicast-IPv4 und/oder IPv6.

mDNS verwendet DNS-A-Records zum Mitteilen von IPv4-Adressen und DNS-AAAA-Records zum Mitteilen von IPv6-Adressen der Geräteschnittstelle im (lokalen) Netzwerk und kann IP-Adressen über DNS-PTR-Records zu Hostnamen auflösen.

DNS-SD verwendet DNS-SRV-Records zur Beschreibung der Dienstzugriffsadressen (z.B. Port-Nummer) und DNS-TXT-Records zur Übermittlung von detaillierteren, kontextabhängigen Dienstzugangsinformationen eines Gerätes im Netzwerk.

mDNS/DNS-SD bietet keinen Schutz vor manipulierten, verzögerten oder ausgespähten mDNS/DNS-SD-Nachrichten. Um einen gewissen Schutz zu erreichen, darf das Protokoll deshalb nur link-lokal und in physisch oder kryptografisch geschützten Netzwerken innerhalb von Liegenschaften verwendet werden.[1] Eine Betrachtung von Angreifer-Modellen zur Privacy von DNS-SD findet sich in [RFC8882].

12.2. Anforderungen

- Das SMGW **KANN** an der HAN-Schnittstelle einen mDNS-Responder nach [RFC6762] implementieren, der dem HAN-Teilnehmern die SMGW-ID nach [DIN43863-5] mitteilt. [REQ.mDNS.Responder.10]
- Sofern der mDNS Response implementiert ist, **MUSS** das SMGW DNS-Anfragen nach "<SMGW-ID>.local." und "smgw.local." mit der link-lokalen Netzwerkadresse des SMGW beantworten. Die <SMGW-ID> wird aus der kanonisierten Geräte-Identifikation nach [DIN43863-5] gebildet. [REQ.mDNS.Responder.20]
- Sofern das SMGW die IPv4 HAN-Schnittstellenadresse nicht durch statische Konfiguration erhalten hat, **SOLL** das SMGW die link-lokale, eindeutige IPv4 HAN-Schnittstellenadresse mittels "Dynamic Configuration of IPv4 Link-Local Addresses“ nach [RFC3927] und ARP-Probes nach [RFC826] bestimmen. [REQ.mDNS.Schnittstelle.10]
- Das SMGW **KANN** die IPv6 IP-Adressvereinbarung nach mit Stateless Address Auto-Configuration (SLAAC) nach [RFC4862] implementieren. [REQ.mDNS.Schnittstelle.20]

[1] Die Authentizität und Vertraulichkeit der Anwendungsdaten der mittels mDNS/DNS-SD bekanntgegebenen Dienste wird durch das TLS-Protokoll gewährleistet.

```
ebsi0012345678.local.
```

Beispiel 12.1. Möglicher DNS-Name des SMGW

12.3. ICS

ICS.mDNS.Responder.10

Der Hersteller **MUSS** im ICS deklarieren, ob mDNS über IPv4 implementiert ist.

ICS.mDNS.Responder.20

Der Hersteller **MUSS** im ICS deklarieren, ob mDNS über IPv6 implementiert ist.

ICS.mDNS.Responder.30

Der Hersteller **MUSS** im ICS deklarieren, ob Dynamische IPv4 Adresskonfiguration nach [RFC3927] implementiert ist.

ICS.mDNS.Responder.40

Der Hersteller **MUSS** im ICS deklarieren, ob Dynamische IPv6 Adresskonfiguration nach [RFC4862] implementiert ist.

13. Netzwerkdiagnoseservice

Dieses Kapitel beschreibt die interoperable Umsetzung eines Netzwerkdiagnoseservices (NDS) zur Bereitstellung von Netzwerkdiagnosedaten durch das SMGW.

13.1. Einordnung des Anwendungsfalls

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[1] 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" 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.

13.2. Funktionsweise

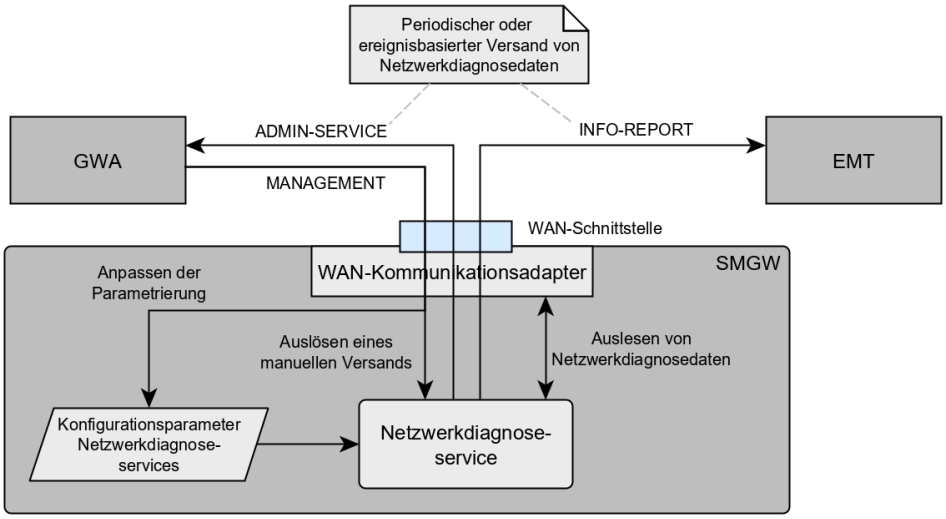

Abbildung 13.1. Übersicht der verwendeten Kommunikationsszenarien

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.

[1] 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.

13.3. Allgemeine Anforderungen

Das SMGW **MUSS** sicherstellen, dass ausschließlich der GWA den Netzwerkdiagnoseservice mithilfe eines Netzwerkdiagnoseprofils (s. ▸Abschnitt 13.5) parametrieren kann. [REQ.NDS.Allgemein.10] Das SMGW **MUSS** mindestens die Parametrierung eines Netzwerkdiagnoseprofils für einen (1) Empfänger unterstützen. [REQ.NDS.Allgemein.20] [2]

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 13.6 an den parametrierten berechtigten Empfänger versenden. [REQ.NDS.Allgemein.30] 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.NDS.Allgemein.40]

Dabei **MUSS** das SMGW den Versand mindestens zu den folgenden Zeitpunkten durchführen können: [REQ.NDS.Allgemein.50]

- Einmalig nach Einspielen eines Netzwerkdiagnoseprofils.
- Einmalig nach Abschluss jedes Startvorgangs des SMGW.
- Einmalig bei Erkennung einer Schwellwertverletzung, wenn das SMGW Schwellwerte implementiert (s. ▸Abschnitt 13.8).
- Periodisch vom letzten Versandzeitpunkt[3] ausgehend im derzeit zu verwendenden Intervall (s. ▸Abschnitt 13.7).
- Einmalig auf Veranlassung des GWA unter Angabe des "Bezeichners" des Netzwerkdiagnoseprofils. Der Versand erfolgt zusätzlich zum periodischen Versand, weshalb der zugehörige Zeitpunkt des Versands nicht als "letzter Versandzeitpunkt" für die Bestimmung der periodischen Versandzeitpunkte berücksichtigt wird.

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 protokollieren. [REQ.NDS.Log.10] Das SMGW **KANN** den Datenverkehr im System-Log protokollieren. [REQ.NDS.Log.20]

ICS.NDS.Log.10

Der GWH **MUSS** im ICS angeben, ob das SMGW den Versand von Netzwerkdiagnosedaten im Logbuch des Anschlussnutzers gemäß ▸REQ.NDS.Log.10 protokolliert.

ICS.NDS.Log.20

Der GWH **MUSS** im ICS angeben, ob das SMGW den Versand von Netzwerkdiagnosedaten im System-Log gemäß ▸REQ.NDS.Log.20 protokolliert.

[2] Die nachfolgende Beschreibung geht von genau einem Empfänger aus. Können Netzwerkdiagnoseprofile für mehrere Empfänger eingebracht werden, gelten die beschriebenen Anforderungen jeweils pro Empfänger.

[3] Ein Versandzeitpunkt gilt auch dann als solcher, wenn der Versand zu diesem Zeitpunkt nicht oder nicht erfolgreich durchgeführt werden konnte.

13.4. Zulässige Netzwerkdiagnosedaten

Das SMGW **DARF** einem berechtigten Empfänger im Rahmen des Versands die Netzwerkdiagnosedaten aus ▸Tabelle 13.1 oder eine Teilmenge davon bereitstellen. [REQ.NDS.Daten.10] Bei Erzeugung einer Datenstruktur für den Versand (s. ▸Abschnitt 13.6) **MUSS** das SMGW den in der Spalte "Attributname" angegebenen Wert für die Identifikation der Daten im Parameter "Werte der Netzwerkdiagnosedaten" verwenden. [REQ.NDS.Daten.20]

Netzwerkdiagnosedatum	Attributname	Datentyp	Beschreibung
Received signal strength indication (RSSI)	"rssi"	Gleitkommazahl in dBm ohne negatives Vorzeichen	Indikator für die Empfangsfeldstärke (Gesamtsignal).
Reference signal received power (RSRP)	"rsrp"	Gleitkommazahl in dBm ohne negatives Vorzeichen	Indikator für die LTE Empfangsfeldstärke (Nutzsignal).
Reference Signal Received Quality (RSRQ)	"rsrq"	Gleitkommazahl in dB ohne negatives Vorzeichen	Indikator für die LTE Empfangsqualität.
Signal-to-noise ratio (SNR)	"snr"	Gleitkommazahl in dB	Indikator für die Signalqualität.
Mobile country code (MCC)	"mcc"	Text	Länderkennung des verwendeten Mobilfunknetzwerks.
Mobile network code (MNC)	"mnc"	Text	Zusammen mit dem MCC eindeutige Identifikation des Funknetzanbieters des verwendeten Mobilfunknetzwerks.
Provider	"provider"	Text	Name des verwendeten Mobilfunkproviders.
Cell ID (CID) der verwendeten Basisstation	"cid"	Text	Eindeutige Identifikation der derzeit verwendeten Basisstation.
Technologie	"technology"	Text	Verwendete Medientechnologie (z.B. Ethernet, LTE).
Betriebsart	"mode"	Text	Betriebsart der verwendeten Technologie (z.B. 100Base-TX).
Frequenzband	"band"	Text	Derzeit verwendetes Frequenzband.
International Mobile Equipment Identity (IMEI)	"imei"	Text	Eindeutige Seriennummer zur Identifikation des Mobilfunkmodems.
International Mobile Subscriber Identity (IMSI)	"imsi"	Text	International eindeutige Mobilfunkteilnehmerkennung.
Integrated Circuit Card Identifier (ICC-ID)	"iccid"	Text	Eindeutige Nummer der SIM-Karte.
Geräteadresse	"linkaddress"	Text	Adresse des medienabhängigen Link-Layers (z.B. MAC-Adresse).
Netzwerkprotokoll	"protocol"	Text	Verwendetes Netzwerkprotokoll (z.B. IPv4, IPv6).
IPv4 Adresse	"ipv4"	Text	Derzeit verwendete IPv4 Adresse des SMGW.
IPv6 Adressen	"ipv6addresses"	Liste von Text	Derzeit verwendete IPv6 Adressen des SMGW.
Betriebszeit WAN	"ifuptime"	Nicht-negative Ganzzahl in Sekunden	Betriebszeit der physischen Schnittstelle des SMGW.

Netzwerkdiagnosedatum	Attributname	Datentyp	Beschreibung
Erfolgreiche Einbuchungen	"successnetlogin"	Nicht-negative Ganzzahl	Anzahl erfolgreicher Einbuchungen bei einem Provider seit letztem Neustart.
Erfolglose Einbuchungen	"failednetlogin"	Nicht-negative Ganzzahl	Anzahl erfolgloser Einbuchungen bei einem Provider seit letztem Neustart.
Übertragenes Datenvolumen (gesendet)	"tx"	Nicht-negative Ganzzahl in Bytes	Gesendetes Datenvolumen in Bytes seit letztem Neustart.
Übertragenes Datenvolumen (empfangen)	"rx"	Nicht-negative Ganzzahl in Bytes	Empfangenes Datenvolumen in Bytes seit letztem Neustart.
Frame Statistik	"frametraffic"	Datenstruktur	Zusammenfassende Historie der ein- und ausgehenden Protocol Data Units des Link-Layers.
Paket Statistik	"packettraffic"	Datenstruktur	Zusammenfassende Historie der ein- und ausgehenden Protocol Data Units des Network-Layers.
Bit Error Rate	"ber"	Gleitkommazahl in Prozent	Aktuell gemessene Bitfehlerrate des Physiscal Layers. Die Zeitdauer, auf die sich die Messung bezieht, wird vom GWH beschrieben.
Round Trip Time	"rtt"	Ganzzahl	Aktuell gemessene Rundlaufzeit (Summe aus Up- und Downstream Latenz) des Link-Layers.

Tabelle 13.1 Zulässige Netzwerkdiagnosedaten

Aufgrund verschiedener Technologien und Modem-Implementierungen können weitere Netzwerkdiagnosedaten vorhanden sein oder andere Begriffe verwendet werden. Das SMGW **DARF** den Versand weiterer Netzwerkdiagnosedaten unter Berücksichtigung von ▸ICS.NDS.Daten.10 unterstützen. [REQ.NDS.Daten.30]

ICS.NDS.Daten.10

Der GWH **MUSS** eine Liste **aller** Netzwerkdiagnosedaten bereitstellen, die das SMGW versenden kann. Für alle Netzwerkdiagnosedaten, die nicht in ▸Tabelle 13.1 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. Die Liste wird im Rahmen der Common-Criteria Zertifizierung überprüft.

13.5. Parametrierung mittels Netzwerkdiagnoseprofil

Der GWA parametriert den Netzwerkdiagnoseservice durch das Einspielen eines Netzwerkdiagnoseprofils über das Kommunikationsszenario MANAGEMENT.

Hierbei **MUSS** das SMGW die Konfigurationsparameter aus der folgenden ▸Tabelle 13.2 im Netzwerkdiagnoseprofil akzeptieren. [REQ.NDS.Parameter.10]

Konfigurationsparameter	Beschreibung
Bezeichner	Im SMGW eindeutiger Bezeichner für das Profil.
Zugeordnetes WAN-Kommunikationsprofil	Referenziert das WAN-Kommunikationsprofil, das für den Versand von Netzwerkdiagnosedaten an einen EMT oder den GWA verwendet wird.
Übertragene Netzwerkdiagnosedaten	Liste zur Auswahl einer Teilmenge von Netzwerkdiagnosedaten, für die Werte verschickt werden sollen (s. ▸Abschnitt 13.4).
Die nachfolgenden Parameter sind optional. Das heißt, der GWA ist im Rahmen der Konfiguration nicht verpflichtet, diese Parameter anzugeben. Wenn die Parameter angegeben werden, muss das SMGW sie jedoch akzeptieren.	
Intervall periodisch	Versandintervall für den periodischen Versand, sofern kein anderes Intervall (nach Start oder Schwellwert) aktiv ist.

Konfigurationsparameter	Beschreibung
Intervall nach Start	Versandintervall für den periodischen Versand nach einem Start bzw. Neustart des SMGW. Wenn der Parameter angegeben ist, muss auch "Gültigkeit Intervall nach Start" angegeben sein.
Gültigkeit Intervall nach Start	Definiert die Dauer nach dem Startvorgang, für die der Konfigurationsparameter "Intervall nach Start" zur Bestimmung der Versandperiode verwendet wird. Wenn der Konfigurationsparameter angegeben ist, muss auch "Intervall nach Start" angegeben sein.
Schwellwerte[4]	Definition von Schwellwerten für einen oder mehrere Konfigurationsparameter aus "Übertragene Netzwerkdiagnosedaten" sowie Angabe der zu überwachenden Richtung (Über- oder Unterschreiten).
Intervall Schwellwert[4]	Versandintervall für den periodischen Versand nachdem ein Schwellwert über- oder unterschritten wurde.
Gültigkeit Intervall Schwellwert[4]	Definiert die Dauer nach dem Beginn des Auftretens einer Schwellwertverletzung, für die der Konfigurationsparameter "Intervall nach Schwellwert" zur Bestimmung der Versandperiode verwendet wird. Wenn der Konfigurationsparameter angegeben ist, muss auch "Intervall Schwellwert" angegeben sein.

Tabelle 13.2 Konfigurationsparameter zur Parametrierung des Netzwerkdiagnoseservices

Eine detailliertere, semantische Beschreibung des zu verwendenden Datentyps NetworkDiagnosticProfile und Vorgaben an die Syntax finden sich in ▸Abschnitt 13.10 und ▸Abschnitt 13.13.

13.6. Datenstruktur zum Versand der Netzwerkdiagnosedaten

Beim Versand von Netzwerkdiagnosedaten **MUSS** das SMGW eine Datenstruktur verwenden, die mindestens die folgenden Elemente enthält: [REQ.NDS.Versandstruktur.10]

Parameter	Beschreibung
Versandauslöser	Gibt den Auslöser für den Versand an. Mögliche Auslöser sind: • Vom GWA ausgelöster Versand • Einspielen des Netzwerkdiagnoseprofils • Start des SMGW • Schwellwertverletzung • Weitere vom Hersteller des SMGW implementierte Auslöser • Periodischer Versand
Geräte-ID des SMGW	Herstellerübergreifende, eindeutige Identifikation des SMGW nach [DIN43863-5].
Zeitpunkt Erstellung	Zeitpunkt zu dem die Datenstruktur erstellt wurde.
Werte der Netzwerkdiagnosedaten	Schlüssel-Werte-Paare aller im Konfigurationsparameter "Übertragene Netzwerkdiagnosedaten" festgelegten Netzwerkdiagnosedaten.

Tabelle 13.3 Verpflichtende Parameter für die übertragene Datenstruktur

Wenn mehrere Versandauslöser gleichzeitig auftreten, **MUSS** das SMGW sicherstellen, dass nur ein Datenversand stattfindet. [REQ.NDS.Versand.10] Die Reihenfolge der Auflistung der möglichen Versandauslöser in ▸Tabelle 13.3 entspricht einer absteigenden Priorität. Das SMGW **MUSS** sicherstellen, dass die Datenstruktur beim Versand den Versandauslöser mit der höchsten Priorität enthält, wenn mehrere Versandauslöser gleichzeitig auftreten. [REQ.NDS.Versand.20]

Eine detailliertere, semantische Beschreibung des zu verwendenden Datentyps NetworkDiagnosticContainer und Vorgaben an die Syntax finden sich in ▸Abschnitt 13.11 und ▸Abschnitt 13.13.

[4] Nur wenn Schwellwerte für Netzwerkdiagnosedaten implementiert werden.

ICS.NDS.Versand.10

Der GWH **MUSS** im ICS angeben, welche Versandauslöser vom SMGW zusätzlich implementiert werden.

13.7. Periodischer Versand

Der periodische Versand von Netzwerkdiagnosedaten verwendet, abhängig von den gesetzten Konfigurationsparametern und den derzeit vorliegenden Bedingungen, unterschiedliche Intervalle zur Bestimmung von Versandzeitpunkten.

Das SMGW **MUSS** das zu verwendende Intervall für den periodischen Versand nach folgendem Ablauf bestimmen: [REQ.NDS.Versand.30]

- Wenn Schwellwerte für Netzwerkdiagnosedaten vom SMGW implementiert werden und das Intervall nach dem Konfigurationsparameter "Intervall Schwellwert" verwendet werden soll (s. ▸REQ.NDS.Schwellwerte.40 in ▸Abschnitt 13.8), dann **MUSS** das SMGW genau dieses Intervall verwenden. [REQ.NDS.Versand.40]
- 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.NDS.Versand.50]
- Wenn der Konfigurationsparameter "Intervall periodisch" angegeben ist, **MUSS** das SMGW genau dieses Intervall verwenden. [REQ.NDS.Versand.60]
- Wenn keine der vorherigen Bedingungen zutrifft, **MUSS** das SMGW den periodischen Versand deaktivieren. [REQ.NDS.Versand.70]

Das SMGW **DARF** den Versand von Netzwerkdiagnosedaten **NICHT** weiter durchführen, wenn das Netzwerkdiagnoseprofil entfernt wurde. [REQ.NDS.Versand.80]

▸Abbildung 13.2 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".

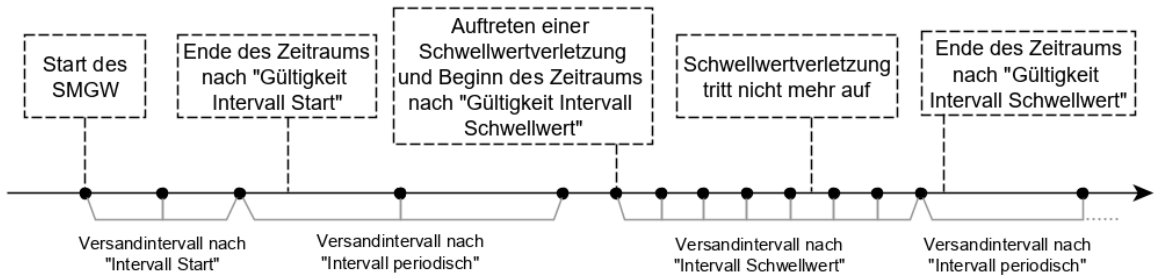

Abbildung 13.2. Beispiel verschiedener Versandzeitpunkte im zeitlichen Verlauf

13.8. 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.NDS.Schwellwerte.10] Wenn der Konfigurationsparameter "Intervall Schwellwert" angegeben ist, **MUSS** das SMGW eben dieses Intervall für den periodischen Versand verwenden. [REQ.NDS.Schwellwerte.20]

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.NDS.Schwellwerte.30]

Das SMGW **MUSS** das Intervall nach Konfigurationsparameter "Intervall Schwellwert" solange verwenden, bis mindestens eine der folgenden Bedingungen erfüllt ist: [REQ.NDS.Schwellwerte.40]

- 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 **MUSS** Schwellwertverletzungen auf Basis des Konfigurationsparameters "Schwellwerte" spätestens zu jedem Versandzeitpunkt erkennen. [REQ.NDS.Schwellwerte.50]

ICS.NDS.Schwellwerte.10

Der GWH **MUSS** im ICS angeben, ob er die Übermittlung von Netzwerkdiagnosedaten auf Basis von Schwellwerten unterstützt.

13.9. Verfügbarkeit im Lebenszyklus

Bezogen auf die Phasen des Lebenszyklus gemäß des Lebenszyklus in [TRv1.1] und [PP-0073] steht die Funktion grundsätzlich in der Phase "Normalbetrieb" zur Verfügung.

REQ.NDS.Lebenszyklus.10

Das SMGW **DARF** den Netzwerkdiagnoseservice **NICHT** in Phasen vor der Personalisierung aktivieren oder einen Versand von Netzwerkdiagnosedaten durchführen.

Der GWH darf den Netzwerkdiagnoseservice in einer Form umsetzen, dass er auch in der Phase "Personalisierung" (Personalization) aktiv sein kann. Dabei muss der GWH die in diesem Kapitel beschriebenen Anforderungen erfüllen. Weiterhin muss der GWH seine Dokumentationspflicht bezüglich der sicheren Auslieferung erfüllen und im Rahmen des CC-Aspekts ALC beschreiben, wie der NetzwerkDiagnoseService gegen Missbrauch und mögliche Angriffe abgesichert ist.

ICS.NDS.Lebenszyklus.10

Der GWH **MUSS** im ICS angeben, ob das SMGW den Netzwerkdiagnoseservice in der Phase "Personalisierung" bereitstellen kann.

REQ.NDS.Lebenszyklus.20

Wenn das SMGW gemäß ▸ICS.NDS.Lebenszyklus.10 keinen Netzwerkdiagnoseservice in der Phase "Personalisierung" anbietet, **DARF** das SMGW **KEINEN** Versand von Netzwerkdiagnosedaten in der Phase "Personalisierung" durchführen.

Sofern der GWH gemäß ▸ICS.NDS.Lebenszyklus.10 den Netzwerkdiagnoseservice in der Phase "Personalisierung" verfügbar macht, muss der GWH die Aktivierung mit dem GWA absprechen. Es dürfen keine GWH-seitigen Voreinstellungen vorliegen, die nicht mit dem GWA abgestimmt sind.

REQ.NDS.Lebenszyklus.30

Das SMGW **DARF KEINEN** Versand von Netzwerkdiagnosedaten durchführen, wenn keine vom GWA bereitgestellte Konfiguration vorliegt.

In Absprache zwischen GWH und GWA darf der Netzwerkdiagnoseservice in der Phase "Personalisierung" (Personalization) für genau einen (1) Empfänger aktiviert werden. Dazu muss der GWA dem GWH die nachfolgenden Elemente authentisch und vertraulich als Teil der initialen Konfigurationsdatei (IKD) übermitteln:

- Netzwerkdiagnoseprofil (gemäß ▸Abschnitt 13.5)
- WAN-Kommunikationsprofil des Empfängers (entfällt bei Versand über Admin-Service, da bereits vorhanden)
- Signatur-, Verschlüsselungs- und TLS-Zertifikat des Empfängers (entfällt bei Versand über Admin-Service, da bereits vorhanden)

Für den Netzwerkdiagnoseservice gelten auch in der Phase "Personalisierung" die Anforderungen dieses Dokuments und zusätzlich die nachfolgenden Anforderungen. Sollte eine der nachfolgenden Anforderungen mit Anforderungen aus anderen Abschnitten in Konflikt stehen, hat die in ▸Abschnitt 13.9 beschriebene Anforderung während der Phase "Personalisierung" den Vorrang.

REQ.NDS.Lebenszyklus.40

Das SMGW **MUSS** dem GWA auch in der Phase "Personalisierung" die Möglichkeit bieten, Netzwerkdiagnoseprofile zu löschen.

REQ.NDS.Lebenszyklus.50

Das SMGW **DARF** dem GWA in der Phase "Personalisierung" **NICHT** die Möglichkeit bieten, Netzwerkdiagnoseprofile zu ändern oder neue Netzwerkdiagnoseprofile einzuspielen.

REQ.NDS.Lebenszyklus.60

Das SMGW **DARF** dem GWA in der Phase "Personalisierung" **NICHT** die Möglichkeit bieten, einen "vom GWA verursachten Versand" auszulösen.

REQ.NDS.Lebenszyklus.70

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.NDS.Lebenszyklus.80

Das SMGW **MUSS** in der Phase "Personalisierung" die Gütesiegelzertifikate des SMGW beim Aufbau von Kommunikationskanälen zum Zweck des Versands von Netzwerkdiagnosedaten verwenden.

REQ.NDS.Lebenszyklus.90

Sofern WAN-Kommunikationsprofile für den Netzwerkdiagnoseservice als Teil der IKD 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.

REQ.NDS.Lebenszyklus.100

Das SMGW **MUSS** in der Phase "Normalbetrieb" die Wirkzertifikate des SMGW beim Aufbau von Kommunikationskanälen zum Zweck des Versands von Netzwerkdiagnosedaten verwenden.

REQ.NDS.Lebenszyklus.110

Das SMGW **MUSS** dem GWA in der Phase "Normalbetrieb" die Möglichkeit bieten, die per initialer Konfigurationsdatei eingespielten Profile zur Konfiguration des Netzwerkdiagnoseservice zu ändern oder zu löschen.

13.10. Datentyp NetworkDiagnosticProfile

Profil zur Parametrierung des Versands von Netzwerkdiagnosedaten an einen Autorisierten Externen Marktteilnehmer (EMT) oder den GWA.

- "id": Enthält die im SMGW eindeutige Identifikation des Profils.
- "physInterface": Eindeutige Identifikation der physischen Schnittstelle, für die ein Versand von Netzwerkdiagnosedaten durchgeführt werden soll.
- "referencedCommunicatonProfile": Enthält den eindeutigen Bezeichner des WAN-Kommunikationsprofils, das zum Versand verwendet werden soll.
- "transferedAttributes[]": Liste von Attributnamen zur Auswahl der zu versendenden Netzwerkdiagnosedaten. Mögliche Werte sind unter anderem "rssi", "snr" oder "imei" aus ▸Tabelle 13.1 sowie weitere vom Hersteller des SMGW festgelegte Attributnamen.
- "intervalPeriodic" (optional): Legt das zu verwendende Versandintervall in Sekunden im Normalfall (keine Schwellwertverletzung, nicht nach dem Start des SMGW) fest. Wenn der Parameter nicht angegeben ist, findet kein periodischer Versand im Normalfall statt.
- "intervalStart" (optional): 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 Parameter nicht angegeben ist, findet kein periodischer Versand im Zeitraum nach dem Neustart statt[5].
- "durationStart" (optional): 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.
- "thresholds[]" (optional): Liste von Schwellwertdefinitionen mit folgenden Parametern:

[5] Dies bezieht sich nur auf den periodischen Versand mit abweichendem Intervall. Der periodische Versand nach "intervalPeriodic" findet, sofern angegeben, statt.

  - "attributeName": Eindeutiger Attributname, der ein Netzwerkdiagnosedatum identifiziert. Der Attributname muss in "transferedAttributes" vorhanden sein.
  - "thresholdValue": Festlegung eines numerischen Werts, dessen Unter- oder Überschreiten eine Schwellwertverletzung darstellt.
  - "upperLimit": Boolescher Wert, der festlegt, ob eine Schwellwertverletzung bei Überschreiten (True) oder bei Unterschreiten (False) des Werts in "threshold" vorliegt.
- "intervalThreshold" (optional): Legt das zu verwendende Versandintervall in Sekunden nach dem Auftreten einer Schwellwertverletzung fest. Wenn der Parameter nicht angegeben ist, findet kein periodischer Versand im Zeitraum nach einer Schwellwertverletzung statt [5].
- "durationThreshold" (optional): 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. Wenn der Parameter nicht angeben ist, wird "intervalThreshold" solange verwendet, bis keine Schwellwertverletzung mehr vorliegt.
- "proprietary" (optional): Weitere Parameter zur Konfiguration des Netzwerkdiagnoseservice, die über die beschriebene Mindestinteroperabilität hinausgeht. Beispielsweise verwendbar zur Definition weiterer Versandzeitpunkte.

```
<?xml version="1.0" encoding="UTF-8"?>
<nds:networkDiagnosticProfile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:bsi:nds nds.xsd" xmlns="http://docbook.org/ns/docbook"
 xmlns:nds="urn:bsi:nds">
    <nds:id>some-profile</nds:id>
    <nds:physInterface>WAN1</nds:physInterface>
    <nds:referencedCommunicationProfile>some-comm-profile-id</nds:referencedCommunicationProfile>
    <nds:transferedAttributes>
        <nds:attribute>rssi</nds:attribute>
        <nds:attribute>mcc</nds:attribute>
        <nds:attribute>mnc</nds:attribute>
        <nds:attribute>imei</nds:attribute>
        <nds:attribute>ipv4</nds:attribute>
        <!-- Example of additional data to be sent -->
        <nds:attribute>mtu</nds:attribute>
    </nds:transferedAttributes>
    <nds:intervalPeriodic>10800</nds:intervalPeriodic>
    <nds:intervalStart>600</nds:intervalStart>
    <nds:durationStart>1800</nds:durationStart>
    <nds:thresholds>
        <nds:threshold>
            <nds:attribute>rssi</nds:attribute>
            <nds:thresholdValue>70</nds:thresholdValue>
            <nds:upperLimit>false</nds:upperLimit>
        </nds:threshold>
    </nds:thresholds>
    <nds:intervalThreshold>15</nds:intervalThreshold>
    <nds:durationThreshold>300</nds:durationThreshold>
    <nds:proprietary>
        <someparameter>42</someparameter>
    </nds:proprietary>
</nds:networkDiagnosticProfile>
```

Beispiel 13.1. NetworkDiagnosticProfile

13.11. Datentyp NetworkDiagnosticContainer

Datencontainer zum Versand von Netzwerkdiagnosedaten an einen Autorisierten Externen Marktteilnehmer (EMT) oder den GWA.

- "trigger": Beinhaltet den Auslöser für den Versand des Datenobjekts. Zulässige Werte sind "ADMIN" (GWA ausgelöster Versand), "CONFIG" (Einspielen des Netzwerkdiagnoseprofils), "REBOOT" (Start des SMGW), "THRESHOLD" (Schwellwertverletzung), "CUSTOM" (weitere vom Hersteller implementierte Auslöser) oder "PERIODIC" (periodischer Versand).
- "gatewayId": Herstellerübergreifende, eindeutige Identifikation des SMGW.
- "physInterface": Eindeutige Identifikation der physischen Schnittstelle, der die Netzwerkdiagnosedaten zugeordnet sind.
- "creationTime": Datum und Uhrzeit der Erstellung des Datenobjekts.
- "data": Liste von Attributname-Werte-Paaren mit folgenden Parametern:
  - "attributeName": eindeutiger Attributname, der ein Netzwerkdiagnosedatum identifiziert.
  - "value": Wert des mittels "key" identifizierten Netzwerkdiagnosedatums.
- "additionalData" (optional): Attributnamen-Werte-Paare von Netzwerkdiagnosedaten, die vom SMGW über die Auflistung in ▸Tabelle 13.1 hinaus versandt werden.

```
<?xml version="1.0" encoding="UTF-8"?>
<nds:ndc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="urn:bsi:nds nds.xsd" xmlns:nds="urn:bsi:nds">
    <nds:trigger>ADMIN</nds:trigger>
    <nds:gatewayId>eABCEE12345678</nds:gatewayId>
    <nds:creationTime>2021-01-15T11:56:52</nds:creationTime>
    <nds:data>
        <nds:rssi>73</nds:rssi>
        <nds:mcc>262</nds:mcc>
        <nds:mnc>99</nds:mnc>
        <nds:imei>012345678901234</nds:imei>
        <nds:ipv4>192.0.2.123</nds:ipv4>
    </nds:data>
    <nds:additionalData>
        <mtu>1500</mtu>
    </nds:additionalData>
</nds:ndc>
```

Beispiel 13.2. NetworkDiagnosticContainer

13.12. Zugriff durch GWA

Das SMGW **SOLL** für den Zugriff zur Verwaltung der Netzwerkdiagnoseservice über den Management-Webservice (WKS1) die URI aus ▸Tabelle 13.4 für den GWA bereitstellen. [REQ.NDS.Zugriff.10]

Das SMGW **SOLL** für die Auslieferung bei Verwendung des Admin-Service Kommunikationsszenarios (WKS2) den Point of Contact gemäß WAN-Kommunikationsprofil verwenden. [REQ.NDS.Zugriff.20]

Das SMGW **SOLL** für die Auslieferung bei Verwendung des Info-Report Kommunikationsszenarios (WKS3) den Point of Contact gemäß WAN-Kommunikationsprofil verwenden. [REQ.NDS.Zugriff.30]

ICS.NDS.Uri.10

Der GWH **MUSS** im ICS angeben, ob seine Implementierung des RESTful Webservice für den Netzwerkdiagnoseservice die URI gemäß ▸REQ.NDS.Zugriff.10 verwendet und vorhandene Abweichungen im ICS beschreiben.

ICS.NDS.Uri.20

Der GWH **MUSS** im ICS angeben, ob das SMGW den Point of Contact aus dem WAN-Kommunikationsprofil gemäß ▸REQ.NDS.Zugriff.20 verwendet und 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.NDS.Zugriff.30 verwendet und vorhandene Abweichungen im ICS beschreiben.

HTTP-Verb	URI	Beschreibung
GET	<PoC>/nds/<id> Request Body: keiner Response Body: NetworkDiagnosticProfile HTTP Statuscode bei Erfolg: 200 Ok	Auslesen eines per <id> identifizierten Netzwerkdiagnoseprofils.
GET	<PoC>/nds/ Request Body: keiner Response Body: Liste von NetworkDiagnosticProfile HTTP Statuscode bei Erfolg: 200 Ok	Auflisten aller eingespielten Netzwerkdiagnoseprofile.
POST	<PoC>/nds/ Request Body: NetworkDiagnosticProfile Response Body: keine Vorgabe HTTP Statuscode bei Erfolg: 201 Created	Einspielen eines neuen Netzwerkdiagnoseprofils.
POST	<PoC>/nds/<id>/triggerSend Request Body: keiner Response Body: keine Vorgabe HTTP Statuscode bei Erfolg: 202 Accepted	Auslösen eines Versands durch den GWA für das per <id> identifizierte Netzwerkdiagnoseprofil.
PUT	<PoC>/nds/{id} Request Body: NetworkDiagnosticProfile Response Body: keine Vorgabe HTTP Statuscode bei Erfolg: 200 Ok	Aktualisieren eines per "id" identifizierten Netzwerkdiagnoseprofils.
DELETE	<PoC>/nds/{id} Request Body: keiner Response Body: keiner HTTP Statuscode bei Erfolg: 204 No Content	Entfernen eines per "id" identifizierten Netzwerkdiagnoseprofils.

Tabelle 13.4 URI für den Zugriff auf die Parametrierung und Funktionen des Netzwerkdiagnoseservices

13.13. XML Schema

Die beiliegende XML Schema Datei nds.xsd enthält den Datentyp NetworkDiagnosticProfile (gemäß ▸Abschnitt 13.10, im Schema als "networkDiagnosticProfile" benannt) zur Parametrierung und den Datentpy Net-

workDiagnosticContainer (gemäß ▸Datentyp NetworkDiagnosticContainer, im Schema als "ndc" benannt) zum Datenversand. Für die Auflistung aller parametrierten Profile zur Parametrierung des Netzwerkdiagnoseservice wird im Schema "networkDiagnosticProfiles" verwendet.

Literaturverzeichnis

[DIN VDE 0418-63-7] *DIN VDE V 0418-63-7 (VDE V 0418-63-7) Messeinrichtungen und -systeme - Teil 63-7: Leitungsgebundene LMN-Protokolle.* 2021 . VDE|DKE K461

[DIN43863-5] *E DIN 43863-5:2012-04 (DIN VDE 0418-63-5) - Herstellerübergreifende Identifikationsnummer für Messeinrichtungen.* 2012 . VDE|DKE K461

[DRAFT-IETF-AFT-SOCKS-SSL-00] *Secure Sockets Layer for SOCKS Version 5.* IETF.

[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 und deren Fernablesung - Teil 4: Zählerauslesung über Funk (Fernablesung von Zählern im SRD-Band.* 2017 . DIN/CEN TC294

[EN13757-7] *DIN EN 13757-7 - Kommunikationssysteme für Zähler - Teil 7: Transport- und Sicherheitsdienste.* 2018 . DIN/CEN TC294

[ISO13239] *ISO 13239 - Information technology -- Telecommunications and information exchange between systems -- High-level data link control (HDLC) procedures.* ISO/IEC JTC 1/SC 6 2002 .

[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-TR-07] *Open Metering System Technical Report 07 - Meter Reading Transmission via M-Bus Compact Profile - Issue 1.0.1.* 2020 . OMS-Group

[OMSS4] *Open Metering System Specification - Volume 2 Primary Communication - Issue 4.3.3.* 2020 . OMS-Group

[PP-0073] *BSI-CC-PP-0073-2014, v1.3.1 Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP.* 2021 . Bundesamt für Sicherheit in der Informationstechnik

[RFC1928] *SOCKS Protocol Version 5.* IETF.

[RFC1950] *ZLIB Compressed Data Format Specification version 3.3.* IETF, L. Peter Deutsch und Jean-Loup Gailly . 1996 .

[RFC1951] *DEFLATE Compressed Data Format Specification version 1.3.* IETF und L. Peter Deutsch . 1996 .

[RFC3274] *Compressed Data Content Type for Cryptographic Message Syntax (CMS).* IETF und P. Gutmann . 2002 .

[RFC3565] *Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS).* IETF und J. Schaad . 2003 .

[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 .

[RFC4862] *IPv6 Stateless Address Autoconfiguration*. IETF. September 2007.

[RFC5083] *Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type*. IETF und R. Housley . 2007 .

[RFC5084] *Using AES-CCM and AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS)*. IETF und R. Housley . 2007 .

[RFC5234] *Augmented BNF for Syntax Specifications: ABNF*. 2008.

[RFC5280] *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. IETF, D. Cooper , S. Santesson , S. Farrell , S. Boeyen , R. Housley und W. Polk . 2008 .

[RFC5480] *Elliptic Curve Cryptography Subject Public Key Information*. IETF, Turner , Brown , Yiu , Housley und Polk . 2009 .

[RFC5639] *Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation*. IETF, Lochter und Merkle . 2010 .

[RFC5652] *Cryptographic Message Syntax (CMS)*. IETF und R. Housley . 2009 .

[RFC6066] *Transport Layer Security (TLS) Extensions: Extension Definitions*. IETF und D. Eastlake . 2011 .

[RFC6762] *Multicast DNS*. IETF. Februar 2013.

[RFC6763] *DNS-Based Service Discovery*. IETF. Februar 2013.

[RFC7230] *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*. IETF, R. Fielding und J. Reschke . 2014 .

[RFC7231] *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content*. IETF, R. Fielding und J. Reschke . 2014 .

[RFC7233] *Hypertext Transfer Protocol (HTTP/1.1): Range Requests*. IETF, R. Fielding , Y. Lafon und J. Reschke . 2014 .

[RFC7616] *HTTP Digest Access Authentication*. IETF. September 2015.

[RFC826] *An Ethernet Address Resolution Protocol*. IETF. November 1982.

[RFC8882] *DNS-Based Service Discovery (DNS-SD) Privacy and Security Requirements*. IETF. September 2020.

[SM-PKI-CP] *SM-PKI-CP - Certificate Policy für die SM-PKI v1.1.1*. 2017 . Bundesamt für Sicherheit in der Informationstechnik

[TR-03109-1-I] *Technische Richtlinie BSI-TR-03109-1, Anlage I: CMS-Datenformat für die Inhaltsdatenverschlüsselung und -signatur, v1.0.9*. 2019 . Bundesamt für Sicherheit in der Informationstechnik

[TR-03109-2] *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-03111] *Technische Richtlinie BSI-TR-03111 v2.10 Elliptic Curve Cryptography*. 2018 . Bundesamt für Sicherheit in der Informationstechnik

[TR-03116-3] *BSI TR-03116-3: Kryptographische Vorgaben für Projekte der Bundesregierung Teil 3 - Intelligente Messsysteme*. Jährlich aktualisiert . Bundesamt für Sicherheit in der Informationstechnik

[TRv1.1] Bundesamt für Sicherheit in der Informationstechnik *Technische Richtlinie TR-03109-1, v.1.1: Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems.* 2021 .

[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

Datenobjekte

In diesem Teil des Glossars finden sich die von den FA verwendeten Datenobjekte.

MTR_LMN_TLS_CRT Das vom SMGW erzeugte X.509 LMN-Zertifikat für die TLS-Kommunikation des Zählers. Das Zertifikat hat die Eigenschaften eines LMN-Zertifikates (s. Detailspezifikation Zertifikatsprofile am LMN) basierend auf [RFC5280].

Das erste TLS-Zertifikat des Zählers wird auch als MTR_LMN_TLS_CRT_0 bezeichnet, während folgende dann mit MTR_LMN_TLS_CRT_1, MTR_LMN_TLS_CRT_2 usw. bezeichnet werden.

GW_LMN_TLS_CRT Das vom SMGW erzeugte, selbstsignierte LMN-Zertifikat des SMGW zur TLS-Kommunikation mit dem Zähler. Das Zertifikat hat die Eigenschaften eines LMN-Zertifikates (s. Detailspezifikation Zertifikatsprofile am LMN). Das erste im SMGW vorhandene LMN-Zertifikat des SMGW wird auch als GW_LMN_TLS_CRT_0 bezeichnet während folgende dann mit GW_LMN_TLS_CRT_1, GW_LMN_TLS_CRT_2 usw. bezeichnet werden.

GWA_WAN_SIG_CRT Das Inhaltsdaten-Signatur-Zertifikat des GWA mit dem Zertifikatsprofil eines C_{Sign}(GWA) nach [TR-03109-4] Anhang A.

SubjectCN Das "commonName" Attribut des X.520 "distinguishedName" Attributes des "Subject"-Datenfeldes eines X.509-Zertifikates. Enthält den Namen des Zertifikatsinhabers.

QueryParameter Liste von Namen und Werten, die bei einer Abfrage zur Selektion von Eigenschaften zur Begrenzung der abgefragten Daten dienen.

GW_HAN_TLS_CRT Das TLS-Authentifizierungszertifikat des SMGW an der HAN-Schnittstelle (s. Detailspezifikation Zertifikatsprofile am HAN) basierend auf [RFC5280] Kapitel 4.

SRV_HAN_TLS_CRT Das TLS-Authentifizierungszertifikat des Servicetechnikers als HAN-Teilnehmer (s. Detailspezifikation Zertifikatsprofile am HAN) mit dem basierend auf [RFC5280] Kapitel 4

CON_HAN_TLS_CRT Das TLS-Authentifizierungszertifikat des Anschlussnutzers (Consumer) als HAN-Teilnehmer (s. Detailspezifikation Zertifikatsprofile am HAN) basierend auf [RFC5280] Kapitel 4

CLS_HAN_TLS_CRT Das TLS-Authentifizierungszertifikat eines CLS-Gerätes als HAN-Teilnehmer (s. Detailspezifikation Zertifikatsprofile am HAN) mit dem basierend auf [RFC5280] Kapitel 4

GWACA_SIG_CRT Das Signaturzertifikat der CA des GWA, die die Zertifikate der Servicetechniker für Diagnose an der HAN-Schnittstelle des SMGW ausstellt (s. Detailspezifikation Zertifikatsprofile am HAN). Das Zertifikat hat die Eigenschaften eines X.509 basierend auf [RFC5280] Kapitel 4

GWHCA_SIG_CRT Das Signaturzertifikat der CA des GWH, die die Zertifikate der Servicetechniker für Diagnose an der HAN-Schnittstelle des SMGW ausstellt (s. Detailspezifikation ⇗ Zertifikatsprofile am HAN). Das Zertifikat hat die Eigenschaften eines X.509 basierend auf [RFC5280] Kapitel 4

Anhang A. Abkürzungsverzeichnis

Abkürzung	Beschreibung
aEMT	Aktiver Externer Marktteilnehmer
AFL	Authentication and Fragmentation Layer, Wireless MBUS
API	Application Programming Interface
APL	Application Protocol Layer, Wireless MBUS
ARP	Address Resolution Protocol
ASN	Abstract Syntax Notation
BER	Basic Encoding Rules (ASN.1)
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CLS	Controllable Local System
CMS	Cryptographic Message Syntax, Inhaltsdatensicherung nach ASN.1
CON	Consumer bzw. Anschlussnutzer
COSEM	COmpanion Specification for Energy Metering
DER	Distinguished Encoding Rules (ASN.1)
DS	Detailspezifikation
EMT	Externer Marktteilnehmer
EnWG	Energiewirtschaftsgesetz
GDEW	Gesetz zur Digitalisierung der Energiewende
GWA	Smart-Meter-Gateway-Administrator
GWH	Smart-Meter-Gateway-Hersteller
HAN	Home Area Network
HDLC	High Level Data Link Control
HKS	HAN-Kommunikationsszenario
HTTP	HyperText Transfer Protocol
IC	Interface Class (für COSEM)
ICS	Implementation Conformance Statement
IETF	Internet Engineering Task Force
IP	Internet Protocol
KS	Kommunikationsszenario
LKS	LMN-Kommunikationsszenario
LMN	Local Meter Network
wM-Bus	Wireless Meter Bus
MessEG	Mess- und Eichgesetz

Abkürzung	Beschreibung
MessEV	Mess- und Eichverordnung
MK	Master Key
MSB	Messstellenbetreiber
MsbG	Messstellenbetriebsgesetz
MTR	Messeinrichtung
N/A	Nicht anwendbar
NTP	Network Time Protocol
OBIS	OBject Identification System (für COSEM)
PSK	Pre-Shared Key, zuvor vereinbarter symmetrischer Schlüssel
PTB	Physikalisch-Technische Bundesanstalt
RFC	Request For Comments
RTT	Round Trip Time
SM	Sicherheitsmodul
SM-PKI	Smart-Meter - Public Key Infrastructure
SMGW	Smart-Meter-Gateway
SML	Smart Message Language
SNI	Server Name Indication
SRV	Servicetechniker des SMGW
TCP	Transmission Control Procotol
TLS	Transport Layer Security, Transportsicherungsprotokoll
TPL	Transport Protocol Layer, Wireless MBUS
TR	Technische Richtlinie
UDP	User Datagram Protocol
UTC	Coordinated Universal Time, Zeitskala
WAN	Wide Area Network
WKS	WAN-Kommunikationsszenario
XML	Extendable Markup Language

Tabelle A.1 In der TR verwendete Abkürzungen