Stellungnahme

zum Entwurf der Technischen Richtlinie TR-03109-1 v1.1

02. August 2021

Vorbemerkung

Bitkom begrüßt den Entwurf der Technischen Richtlinie Version 1.1 (TR), der im Wesentlichen die bisherigen Anforderungen konsolidiert und den systemischen Ansatz stärkt. Zur raschen Fortsetzung der Digitalisierung der Energiewende und zur Nutzung der sicheren IKT für weitere Anwendungsfälle sollte der Entwurf zeitnah verabschiedet und die darauf aufbauenden Zertifizierungen durchgeführt werden. Eine strukturierte Weiterentwicklung im Rahmen des Stufenplans ist in den nächsten Versionen unter Einbeziehung der Verbände und der Branchenerfahrung vorzunehmen.

Der Entwurf, der die Grundlage für die nach OVG-Urteil und resultierender MsbG-Anpassung geforderte Zertifizierung nach der Technischer Richtlinie bildet, spiegelt insbesondere die Bedeutung der kommunikativen Anbindung und der informationstechnischen Systeme für die Digitalisierung der Energiewende wieder, die gemeinsam und systemisch die definierten Anforderungen realisieren.

Es wird klar, dass die hohen Sicherheitsstandards, die in den Systemlandschaften in den vergangenen Jahren schon eingeführt und umgesetzt wurden, wesentlich zum Erfolg der gesamten Infrastruktur beitragen.

Mit der Verabschiedung der Technischen Richtlinie Version 1.1 wird die Unsicherheit, die durch das OVG-Urteil in der Branche entstanden ist, abschließend ausgeräumt und durch die geschaffene Rechtssicherheit dringend notwendige Investitionen in die Messsystem-Infrastruktur und die Weiterentwicklung der IKT-Strukturen begünstigt. Besonders zu befürworten ist dabei die Etablierung des nach MsbG vorgesehenen Ausschusses Gateway-Standardisierung und die breite Einbeziehung der Verbände bei der Festlegung von Anforderungen. Durch die Einbeziehung aller relevanten Interessensgruppen wird das Erzielen eines optimalen Ergebnisses und die breite Akzeptanz gesichert, da die unterschiedlichen Perspektiven zur hohen Qualität der beschlossenen Rahmenbedingungen beitragen.

Besonders zu begrüßen sind die Optionen und eingeräumten Freiheitsgrade für ein Netzwerk-Management der WAN-Komponenten eines SMGWs innerhalb und außerhalb des TOEs nach BSI-Protection Profile. Der Betrieb von SMGW in Weitbereichs-Kommunikationsnetze ohne diese Funktion ist nicht effizient möglich. Dass die Kommunikationsnetze und -komponenten der SMGWs auf gängige, internationale Standards aufsetzen, ist sehr zu begrüßen und wird auch dringend benötigt. Gerade im systemischen Kontext ist die Weitbereichskommunikation und das Management der Kommunikationsanbindung eine essenzielle Voraussetzung für die Verfügbarkeit von Diensten und die Grundlage für Mehrwert und Nutzen.

Die Weiterentwicklung der Technischen Richtlinie in den auf Version 1.1 folgenden Versionen sollte entlang des Stufenmodells und zusammen mit den Verbänden und der Branche vorgenommen werden. Neue Versionen können ausgehend von der expliziten Definition der Anforderungen und der formalisierten Struktur deutlich besser und

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Sebastian Schaule
Referent Energie
T +49 30 27576-204
s.schaule@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

transparenter ausgearbeitet werden als in den vorherigen Versionen 1.0 bzw. 1.0.1, in denen Anpassungen über Errata-Dokumente ausgesteuert werden mussten. Festzuhalten bleibt aber, dass der Entwurf der Version 1.1 ohne Anpassungen verabschiedet werden sollte und Anpassungswünsche in einem „Themenspeicher" zusammen mit den Anforderungen aus der folgenden Stufe des Stufenmodell konsolidiert und erst dann in die Folgeversion der TR eingearbeitet werden sollte, wodurch ein konsistentes Anforderungsprofil gewährleistet ist.

Bitkom und die beteiligten Unternehmen engagieren sich seit vielen Jahren für sichere Digitalisierung auch in der Energiewirtschaft. Nur mit dem Einsatz dieser Technologien sind Energie- und Verkehrswende, das Ziel der CO_2-Neutralität bei gleichbleibend hoher Versorgungssicherheit sowie Akzeptanz in der Bevölkerung zu erreichen. Der Entwurf der Technischen Richtlinie Version 1.1 stellt einen wichtigen Schritt auf dem Weg in diese Richtung dar, schafft Planungs- und Rechtssicherheit und macht den weiteren Weg für Entwicklung und Innovation frei. Bei der Weiterentwicklung des BSI/BMWI-Stufenmodells und der Überführung in kommende Versionen der Technischen Richtlinie trägt Bitkom gerne bei und bringt sich weiterhin entsprechend ein.

Im Einzelnen:

2.1. Akteure am SMGW

Auch Gebäudeeigentümer/Anschlussnehmer sind relevante Akteure am SMGW und sollten in die Auflistung aufgenommen werden. Sie sind Inhaber der Gebäudeversorgungsanlagen, vergeben die Betriebsführung und sind Vertragspartner des Netzbetreibers im Netzanschlussvertrag. Zudem entscheiden sie über sämtliche bauliche Veränderungen im Gebäude durch Dritte.

Zu 2.1.1. Anschlussnutzer

Folgender Satz im ersten Absatz solle ersetzt werden:

Technischer Akteur am SMGW, der elektrischen Energie, Gas, Wasser oder Wärme bezieht oder erzeugt und zur Nutzung des Netzanschlusses berechtigt ist. ~~Der Anschlussnutzer verwendet zur Interaktion mit dem SMGW ein Kommunikationsgerät (z.B. Display).~~ Das SMGW stellt Anschlussnutzern wie Anlagenbetreibern und Anschlussnehmern Betriebsdaten an der HAN-Schnittstelle eines SMGW zur Verfügung. Diese Schnittstelle ermöglicht ferner Letztverbrauchern den Zugang zu Verbrauchsdaten. Der technische Akteur Anschlussnutzer ist beispielsweise ein Letztverbraucher oder Anlagenbetreiber gemäß [MsbG].

Zu 2.2. Schnittstellen und Funktionen des SMGW

Der erste Satz auf Seite 7 sollte abgeändert werden:

Heimnetz (Home Area Network, HAN): Im HAN ~~des Anschlussnutzers~~ eines oder mehrerer Anschlussnutzer kommuniziert das SMGW mit den steuerbaren Energieverbrauchern bzw. Energieerzeugern (CLS, also z.B. private Ladeeinrichtungen, Kraft-Wärme-Kopplungs- oder Photovoltaik-Anlagen).

Zu 3.2.2.1. WAF1: Administration und Konfiguration

Auf Seite 15 zu den Unterpunkten bei CLS-Proxy Verwaltung:

- *Das SMGW SOLL* dem GWA das Initiieren einer Proxy-Kommunikationsverbindung zwischen aktivemEMT und CLS anbieten. [REQ.WAN.Management.100]*

- *Das SMGW SOLL* dem GWA das Beenden einer Proxy-Kommunikationsverbindung zwischen aktivemEMT und CLS anbieten. [REQ.WAN.Management.110]*

*Anmerkung: Wenn Anlegen, Aktualisieren und Löschen von Profilen MUSS-Optionen sind, dann sollten auch Initiieren und Beenden einer Proxy-Kommunikationsverbindung MUSS-Optionen sein. Sollten diese SOLL-Optionen bleiben, Bitte um Information, welche Begründungen akzeptiert werden.

[…]

Auf Seite 16 sollten unter Schlüssel-/Zertifikatsmanagement folgende Punkte jeweils ergänzt werden:

- *Das SMGW MUSS dem GWA das Aktualisieren seiner GWA-Zertifikate, der EMT-Zertifikate und der SubCA-Zertifikate anbieten. [REQ.WAN.Management.190]*
  […]
- *Das SMGW MUSS dem GWA die Aktualisierung der SMGW-LMN-Zertifikate und der zählerindividuellen Schlüssel MK anbieten. [REQ.WAN.Management.210]*

Zu 3.2.3. Kommunikationsszenarien

Bitte um Definition der Inhaltsdaten in Tabelle 3.1 (Kommunikationsszenarien an der WAN-Schnittstelle):

a) Sind Inhaltsdaten definiert als beliebige Daten, dann müsste Tabelle 3.1 analog zu den Tabellen 3.2-3.6 so aussehen, da auch Responses und Verbindungsabbau empfangen werden:

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

b) Sind Inhaltsdaten definiert als verschlüsselungspflichtige Daten im HTTP-Body, d.h. CMS-Container, dann müsste die Tabelle folgendermaßen aussehen, da nicht verboten ist, dass der EMT Daten zurücksendet:

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

Zu 3.2.5. Kommunikationsprofile für die WAN-Kommunikation

In Tabelle 3.9 bitte EMT_WAN_ENC_CRT zu EMT_WAN_SIG_CRT korrigieren:

Zertifikat des Kommunikationspartners für die Signierung der Inhaltsdaten	*GWA_WAN_SIG_CRT oder EMT_WAN_~~ENC~~SIG_CRT*	*Das Zertifikat des GWA oder EMT für Signierung von Inhaltsdaten, die vom GWA oder EMT durchgeführt werden muss.*

Zu 3.2.6.4. Zeitsynchronisation-Protokoll

Anmerkung: Sowohl REQ.WAN.Zeitsynchronisation.30 als auch ICS.WAN.Zeitsynchronisation10 können von einem SMGW nicht gewährleistet werden. Da ein einzelnes SMGW nichts von den Strategien der anderen SMGWs weiß, kann es immer zu gleichzeitigen NTP-Anfragen sowie Retries kommen.

Zu 3.2.6.5. Transport von TLS

Für eine standardisierte Implementierung des Punktes...

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

... müsste die TR-03109-1-WAN TLS-Client Funktionalität mit ServerNameIndication RC1-20.10.2017 finalisiert werden.

Zu 3.3.4.2. Sicherung der LMN-Kommunikation mit symmetrischen Verfahren

In der BSI-TR-03116-3 Kap. 7 soll MK wohl für Meter Key stehen, hier wird als Langform für MK Master Key genannt.

Zu 3.4.2.1. HAF1: Bereitstellung von Daten für den Anschlussnutzer

Absatz 1 bedarf folgender Ergänzung:

Das SMGW bietet eine Schnittstelle im HAN (if_GW_CON) an, über die das SMGW dem berechtigten Anschlussnutzer seine Messwerte und andere für ihn relevante Informationen bereitstellt, um sie beispielsweise über eine Anzeigeeinheit zur Rechnungsprüfung zu visualisieren. Weiterhin ist die Verarbeitung aus dem HAN (if_GW_CON) durch ein anderes (CLS-)Gerät im HAN Bereich zu ermöglichen. Als Anzeigeeinheit kann zur Rechnungsprüfung ein Gerät mit Transparenz- und Display-Software nach [MessEG]/[MessEV] verwendet werden.

Zu 3.4.3.4. Kommunikationsszenario HKS4: Transparenter Kommunikationskanal initiiert durch aktiven EMT

Der erste Punkt des Ablaufs...

a. *Der aktive EMT teilt die gewünschte Zieladresse des CLS dem GWA (z.B. über einen Webservice) mit. Die Schnittstelle aktiver EMT - GWA wird nicht durch diese TR festgelegt.*

... ist nicht Teil dieser TR. Welche Spezifikation wird diese Schnittstelle definieren?
Die Dringlichkeit für diesen ersten Punkt des Ablaufs ist hoch.

Zu 3.4.4. Sicherung der Kommunikationsverbindungen in das HAN

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

Anmerkung: Wer darf selbstsignierte Zertifikate in das SMGW einbringen? Wie wird die Vertrauenswürdigkeit der Kommunikationspartner sichergestellt?
BTW, Zertifikate, die aus der SM-PKI stammen, sind außer dem Root-Zertifikat nie selbstsigniert.

Zu 3.4.4.1. Sicherung der Kommunikation mit dem Anschlussnutzer / Servicetechniker

Anmerkung zu Abs. 5 [REQ.HAN.SicherungKommunikationConSrv.70]:

Hier sollte zwischen IF_GW_CON, IF_GW_CLS und IF_GW_SRV getrennt werden. Alternativ nach der Zugriffsmethode ID+Passsword und TLS-Client.
I&A-Fehler am IF_GW_CON dürfen IF_GW_CLS nicht blockieren, ansonsten ist hier eine DoS-Attacke gegen CLS möglich.

Zu 4.5. Anforderungen an Berechtigungen

Der Abschnitt „Anforderungen und Berechtigungen“ ist keine Detaillierung zu „4. Messwertverarbeitung“. Der Abschnitt sollte entweder unter 3.5. oder als eigenes Kapitel 5 gefasst werden.

Zu 4.5.3. Smart-Meter-Gateway-Administrator

Anmerkungen zu folgenden Unterpunkten:

- *Das SMGW MUSS sicherstellen, dass der GWA das Eichtechnische Log und das System-Log nicht ändern* kann. [REQ.WFA.GwaZugriff.80]*

  *Anmerkung: Beim System-Log ist ein Überschreiben der ältesten Einträge durch neue Einträge möglich (Ring-Speicher). Die Größe vom Ring-Speicher kann vom GWA geändert werden. Ein gezieltes Löschen oder Ändern von Einträgen ist nicht möglich.

- *Das SMGW MUSS sicherstellen, dass der GWA die Anschlussnutzer-Logs der Anschlussnutzer nicht einsehen oder ändern** kann. [REQ.WFA.GwaZugriff.90]*

  **Anmerkung: Ein GWA kann ein Anschlussnutzer und dessen Logs nur komplett löschen. Der GWA muss dabei aber Vorhaltefristen beachten.

Zu 4.5.6. Externe Marktteilnehmer

Das SMGW MUSS sicherstellen, dass EMT keinen direkten Zugriff auf Messwertlisten haben, sondern Messwerte ausschließlich entsprechend der Berechtigungen der konfigurierten Auswertungsprofile (s. Abschnitt 4.2) vom SMGW an den EMT versendet werden. [REQ.WFA.EmtZugriff.20]

Anmerkung: Das SMGW MUSS sicherstellen, dass ein aktiver EMT nur über einen CLS-Proxy Kanal zu den jeweiligen EMT zugeordneten CLS kommunizieren kann.

Zu 5. Weitere Funktionale Anforderungen

Bitte keine Anforderungen aus dem SMGW PP-0073 duplizieren.

Anmerkungen zu den Detailspezifikationen

Zu 3.1 Einleitung

Tabelle 3.1 Zertifikatsprofiltypen der LMN-Zertifikate bedarf folgender Ergänzung:

Zertifikatstyp	***Zertifikats-Profiltyp***	***Aussteller***
GW_LMN_TLS_CRT	*Selbst-Signiert*	*SMGW*
MTR_LMN_TLS_CRT	*Selbst-Signiert*	*SMGW bzw. MTR-Hersteller**

*Anmerkung: Siehe TR-03116-3, Abschnitt 6.3.1
"Für Zähler, die TLS unterstützen, MUSS das initiale Schlüsselpaar vom Hersteller oder vom Smart Meter Gateway erzeugt und authentisch in den Zähler eingebracht werden."

Ein Hersteller hätte durchaus Interesse daran, seine MTR-Zertifikate eindeutig identifizierbar aus seine Produktions-PKI zu erstellen. Ein anschließender Zertifikatsaustausch auf das vom SMGW erstellte MTR "Wirk" Zertifikat könnte trotzdem stattfinden.

Zu 3.3.3. Issuer und Subject

- ~~*Das Namensschema für den "commonName" der LMN-Teilnehmer lehnt sich an [SM-PKI-CP] Anhang A an.*~~**

  **Anmerkung: Das Namensschema der SM-PKI-CP ist eben nicht zutreffend. Es sollte das bisherige Namensschema "<DIN43863-5-HUID>.sm" bzw. "<MAC/EUI>.eui" verwendet werden. Siehe auch 3.3.5.3. SAN.

  […]

- *Es wird zwischen den Funktionsrollen SMGW und MTR unterschieden.* ~~*Zur Bildung des commonName wird die Funktionsrolle an die Identifikation des Gerätes nach [DIN43863-5] angehängt.*~~***

  ***Anmerkung: Diese Rolle wird bereits durch den ersten Buchstaben der DIN43868-5 HUID definiert.

- *Das Zertifikat hat außer dem "commonName" keine weiteren Distinguished Name Attribute.* ~~*Diese Anforderung schließt aus, dass das Zertifikat aus der SM-PKI stammt.*~~****

  ****Anmerkung: Eigener Spiegelpunkt: "Die LMN-Zertifikate (SMGW und MTR) stammen nicht aus der in [TR-03109-4] definierten SM-PKI!"

Zu 3.3.5. Extensions

Nr.	*Bezeichnung*	*MTR_LMN_TLS_CRT Element vorhanden*	*GW_LMN_TLS_CRT Element vorhanden*
1	*AuthorityKeyIdentifier*	*x*	*x*
2	*SubjectKeyIdentifier*	~~*x*~~*	~~*x*~~*
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*	*x***	*x***
10	*CRLDistributionPoints*	*x*	*x*

*Anmerkung: Optional
**Anmerkung: r Recommended. Zusätzlich zur KU könnten auch die EKU TLS-Client und TLS-Server gesetzt werden. Siehe auch 4.3.5.4 ExtendedKeyUsage.

Zu 3.3.5.2. BasicConstraints

- *Extension-ID (OID): 2.5.29.19*
- *Kritisch: Ja*
- *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": TRUE~~**
- *~~"pathLenConstraint": 0~~**

**Anmerkung: Das Zertifikat ist ein End-Entity und stellt keine Zertifikate aus. Das Zertifikat darf in einem Truststore eben nicht als CA erkannt werden. Pathlen=0 macht dazu keine Einschränkung. => BC-cA: False, ohne PathLength.

Zu 3.3.5.3. SubjectAltName

- *"dNSName": Es wird empfohlen, die eindeutige Kennung von SMGW oder der Messeinrichtung basierendauf [DIN43863-5] als Domain Name Label mit angehängtem ".smgw", ".mtr"* zu formatieren.*

**Anmerkung: Empfehlung das bisherige Hostnamensschema "<DIN43863-5 HUID>.sm" bzw. "<MAC/EUI>.eui" zu verwenden.

[...]

Der Fall...

Sofern Issue und Subject leer sind, muss die SubjectAltName Extension gemäß [RFC5280] vorhanden sein.

...kann nicht eintreten, da Issuer und Subject gemäß Tabelle 3.4 Pflichtfelder sind und über Namenskonventionen nicht leer sein dürften. Die Anforderung kann unseres Erachtens nach entfernt werden.

Zu 3.4.2. Issuer und Subject

Für Zertifikate der Messeinrichtung gilt für die Bildung des SubjectCN die Bildungsregel ~~<id>.<func> [.<ext>].~~

- *~~Funktionsbezeichnung (<func>) enthält den Text "MTR" oder "mtr".~~**
- *Die Identifikation (<id>) enthält die herstellerübergreifende Identifikationsnummer für Messeinrichtungen nach [DIN43863-5] mit der Sparte "1" (Elektrizität), "6" (Wärme), "7" (Gas), "8" (Kaltwasser), oder"9" (Heißwasser).*
- *~~Die Erweiterung [<ext] entfällt zunächst.~~*

**Anmerkung: Siehe SubjectAltName.

Zu 3.5.2. Issuer und Subject

Für Gateway-Zertifikate gilt für die Bildung des SubjectCN die Bildungsregel ~~<id>.<func>[.<ext>].~~

- ~~*Funktionsbezeichnung (<func>) enthält den Text "SMGW" oder "smgw".**~~
- *Die Identifikation (<id>) enthält die herstellerübergreifende Identifikationsnummer für Messeinrichtungen nach [DIN43863-5] mit der Sparte "E".***
- ~~*Die Erweiterung [.<ext>] entfällt zunächst.*~~

*Anmerkung: Siehe SubjectAltName.
**Anmerkung: Die HUID im Zertifikat sollte komplett in Lower-Case, ohne Leerzeichen kodiert werden.

Zu 3.5.3. Beispiel

Certifcate:
Data: Version: 3 (0x2)
Serial Number: e8:a5:fe:ee:52:36:de:56
Signature Algorithm: ecdsa-with-SHA256
*Issuer: CN = ebsi0012345678.~~smgw~~**

[...]

X509v3 extensions:
X509v3 Basic Constraints:
*CA:~~TRUE~~** X509v3*

*Anmerkung: .sm
** Anmerkung: FALSE

Zu 4.1. Einleitung

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

*Anmerkung: Typ A heißt, dass es sich hier um selbstsignierte Zertifikate handelt.
Wie sind die Sicherheitsanforderungen zur Absicherung der HAN-Schnittstelle durch Zertifikate des Typs A? Insbesondere: Müssen die privaten Schlüssel auf einem HSM liegen?

**Anmerkung: oder einen anderen CA-Dienstleister.
GWH ist nicht der Hersteller von CLS. GWA ist nicht der Betreiber bzw. Admin von CLS (=> zuständige aktiver EMT) Kundenzugänge (ID+Password oder TLS-Zertifikat) werden vom zugehörigen EMT verwaltet.

[...]

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

Anmerkung (zur ganzen Tabelle): Tabelle 4.1 gibt an, dass insbesondere Consumer und Servicetechniker sich die Zertifikate selbst ausstellen. Damit wäre jeder ein Consumer oder Servicetechniker, der es sein will…

*Anmerkung: Hier wäre ein Typ-B-Zertifikat hilfreich gewesen, welches von den HAN-Teilnehmern bzw. dessen Admin auch überprüft und validiert werden könnte und somit eindeutig nachweist, dass es hier um SMGW 12345 von Hersteller XYZ handelt.

**Anmerkung: Auch hier kann das Zertifikat von anderen Marktteilnehmer ausgestellt werden, z.B. mein MSB/LF (i.e. ein EMT). EMS-Display Hersteller (i,e, ein MFR).

***Anmerkung: Auch das CLS_HAN_TLS_CRT kann von Typ B CLS-Hersteller CA sein.

****Anmerkung: Auch mehrstufigen CA-Hierarchien sind hier möglich/zulässig. Die CA-CertChain wird nur bei der Validierung vom Zertifikat vor der Konfiguration benötigt. Danach ist die CA durch den DirectTrust vom EE-Zertifikat irrelevant. Der GWA bzw. der EMT-CLS Admin muss Sperrungen entsprechend zeitnah auf dem SMGW bzw. CLS abbilden.

*****Anmerkung: GWH ist kein CLS-Hersteller. =>Manufacturer-CA MFR_CA
Eine GWH_CA könnte optional SRV_HAN_TLS_CRT ausstellen.

Zu 4.2. Laufzeit

Eine Prüfung der zeitlichen Gültigkeit von selbstsignierten (Typ A) Zertifikaten durch das SMGW wird nichtvorgegeben, 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.*

*Anmerkung (Fußnote zur Erläuterung): Geräte im HAN haben bei der Inbetriebnahme initial oft keine korrekte synchronisierte *Datum+Uhrzeit*. Die Zeitangaben im selbstsignierten Zertifikat können somit stark von der aktuellen SMGW-Zeit abweichen, d.h. eine Prüfung der zeitlichen Gültigkeit ist hier nur sehr eingeschränkt möglich.

[…]

Das SMGW MUSS die zeitliche Gültigkeit von kurzlebigen SRV_HAN_TLS_CRT Zertifikaten vom Typ B und von ~~GWACA_SIG_CRT~~-Zertifikaten prüfen. [REQ.ZertifikateHAN.Allgemein.20]*

*Anmerkung: "kurzlebig" ist nicht definiert.
=> Praxis: Gültigkeitsdauer 2 bis 3 Jahre.

Anmerkung: dessen "*_CA_SIG_CRT"

[...]

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).

Anmerkung: Bedeutet dies, dass bei Laufzeit "0" die Validierung des Zeitpunktes notAfter des Feldes Validity entfällt?

Zu 4.3. Zertifikatsstruktur, Tabelle 4.4 Struktur des Elementes "TBSCertificate"

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: ~~GWA-ID oder GWH-ID~~**

*Anmerkung: Subject-DN der ausstellende CA.

Zu 4.3.5. Extensions

BasicConstraints	*~~r cA=TRUE, pathLenConstraint=0~~**	*m cA=FALSE, pathLenConstraint=1***

Tabelle 4.5 Extensions
*Anmerkung: Das Zertifikat ist ein End-Entity und stellt keine Zertifikate aus. Das Zertifikat darf in einem Truststore eben nicht als CA erkannt werden. Pathlen=0 macht dazu keine Einschränkung.
=> BC-cA: False, ohne PathLength.

**Anmerkung: PathLen ist obsolete bei cA=False
(CA=True + pathLen=0 für die CA darüber)

Zu 4.3.5.1. KeyUsage

- *Gesetzte Bits: digitalSignature(0)**

*Anmerkung: Weitere KUs sind für das CLS-Device möglich, falls dieses Zertifikat auch für Inhaltsdatenkrypto verwendet wird. Das SMGW-HAN-Zertifikat hat nur das KU-digSig gesetzt.

Zu 4.3.5.3. SubjectAltName

- *"dNSName": Es wird empfohlen, die eindeutige Kennung von SMGW oder HAN-Teilnehmer basierend auf[DIN43863-5]* als Domain Name Label zu formatieren.*

*Anmerkung: Nicht alle HAN-Teilnehmer haben eine DIN43863-5 HUID.
Empfehlung das bisherige Namensschema [DIN43863-5].sm bzw. [MAC/EUI].eui zu verwenden.
Für CON_HAN_TLS_CRT könnte die Messlokations-ID herangezogen werden.
Für SRV_HAN_TLS_CRT könnte die Konzessionsnummer vom Techniker/Betrieb verwendet werden.

[...]

Der Fall...

Sofern Issue und Subject leer sind, muss die SubjectAltName Extension gemäß [RFC5280] vorhanden sein.

...kann nicht eintreten, da Issuer und Subject gemäß Tabelle 3.4 Pflichtfelder sind und über Namenskonventionen nicht leer sein dürften. Die Anforderung kann unseres Erachtens nach entfernt werden.

Zu 4.3.5.4. ExtendedKeyUsage

- *Beschreibung: ~~Die Extension ExtendedKeyUsage (spezifiziert in [RFC5280], 4.2.1.12) gibt an, ob es sich beidem gegebenen Zertifikat um ein TLS-Zertifikat handelt.~~**

*Anmerkung: In der EKU Extension (RFC5280, 4.2.1.1.12) kann angegeben werden, ob das Zertifikat als TLS-Client und/oder TLS-Server Zertifikat genutzt werden kann.

Zu 4.4.2. Namensschema der SMGW-HAN-Zertifikate

Attribut Typ	***Kürzel***	***Vorgabe***	***Wert***	***Erläuterung***
common name	*CN*	*r*	*"<id>.~~SMGW~~"* *	*<id> Herstellerübergreifende Identifikationsnummer für Messeinrichtungen nach [DIN43863-5] mit der Sparte "E".*
organisation	*O*	*o*	*"<O>"*	*Das Zertifikat stammt nicht aus der SM-PKI.***
organisational-unit	*OU*	*~~R~~****	*"<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 bis2^31-1 und startet bei 1. Diese wird bei jedem neuen Zertifikat um den Wert 1 hochgezählt.*

*Anmerkung: ".sm"

**Anmerkung: Falls verwendet darf das Feld "SM-*PKI" nicht enthalten.

*** Anmerkung: o Optional
Empfehlung das Feld nicht zu verwenden.

Zu 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>[.<func>[.<extension>]]"*	• *<func> **MUSS** für TLS-Proxy Nutzer ("CLS") gleich" CLS" sein. In diesem Fall enthält <id> die 14-stellige herstellerübergreifende Identifikationsnummer für Messeinrichtungen nach [DIN43863-5] oder eine andere auf der Komponente des HAN-Teilnehmers lesbare, praktisch eindeutige, nicht-wechselnde, herstellerübergreifende Netzwerkschnittstellenadresse, die nicht mit der Identifikation nach[DIN43863-5] verwechselt werden kann.**** • *<func> **MUSS** für Servicetechniker gleich "SRV" sein. In diesem Fall enthält <id> ein vom GWA vergebenes Pseudonym des SRV.*****
organisation	*O*	*o*	*"<O>"*	*Das Zertifikat stammt nicht aus der SM-PKI (Darf nicht mit "SM-" beginnen)******
organisational-unit	*OU*	*o*	*"<OU>"*	*-*
country	*C*	*o*	*"<LC>"*	*Zwei Zeichen Ländercode gemäß [ISO 3116 ALPHA-2]*
serial number	*SERIAL-NUMBER*	*o*	*"<SN>"*	*Sequenznummer des Zertifikats******* im Bereich von 1 bis2^31-1. 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 ~~enthält keine weiteren Attribute.~~*********

*****Anmerkung: Nicht alle HAN-Teilnehmer haben eine DIN43863-5 HUID.
Empfehlung das bisherige Namensschema [DIN43863-5].sm bzw. [MAC/EUI].eui zu verwenden.
Für CON_HAN_TLS_CRT könnte die Messlokations-ID herangezogen werden.
Für SRV_HAN_TLS_CRT könnte die Konzessionsnummer vom Techniker/Betrieb verwendet werden.

******Anmerkung: Das Zertifikat wird in der Regel nicht vom GWA ausgestellt. Die SRV-Zertifikate werden dem GWA zur Konfiguration auf dem SMGW bereitgestellt.
Vorgabe: Die Nutzung eines SRV Zertifikats muss eindeutig der Tätigkeit einer Person zugeordnet werden können. Ein Zertifikat kann aber von abwechselnden Personen genutzt werden.

*******Anmerkung: Darf somit nicht "SM-*PKI" enthalten.
Die Zuordnung zur SM-PKI wird über den CA gemacht, Der Inhalt vom DN-O Feld ist dazu irrelevant.

bitkom

****Anmerkung: Falls vorhanden enthält das Feld die Sequenznummer des ....

*****Anmerkung: Darf weitere Attribute enthalten (nicht empfohlen).

Zu 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
*~~Es wird angenommen, dass die CA in der vertrauenswürdigen Umgebung des zertifizierten GWA gemäß[TR-03109-6] bzw. des zertifizierten GWH gemäß [PP-0073] betrieben wird und die Anforderungen an die Erzeugung und Speicherung von Schlüsselpaaren der CA und der Servicetechniker das für die Teilnahme an der SM-PKI erforderliche Niveau besitzt.~~**

***Anmerkung: Diese Annahme ist so nicht gegeben und stellt neue Anforderungen an den GWA, EMT bzw. GWH-Betriebsprozesse.
Der GWH kann in Rahmen der SMGW-CC-Zertifizierung über die Guidance-Dokumente verbindliche Anweisungen für den zertifizierten Betrieb machen. Dazu gehört auch die Konfiguration von HAN-Profilen mit den CLS-, SRV- und CON-Zertifikaten. Es wäre möglich, hier Sicherheitsanforderungen an die Erstellung dieser Zertifikate zu stellen.

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

Anmerkung: Abschnitt komplett streichen.

Die Inhalte der CA-Zertifikate richten sich nach PKIX RFC-5280, mit der Empfehlung die genutzte PKI an den SM-PKI-Vorgaben auszurichten.

Zu 5.2. Anforderungen

Bedeutet die Anforderung ...

Die Implementierung MUSS Zertifikate nach [RFC5280] Kapitel 4.1 verarbeiten und validieren. [REQ.CMS.Implementierung.30]

... implizit, dass auf dem CLS-Kanal CMS als Protokoll verwendet werden muss?

Zu 9.2. Anforderungen

Anmerkung: Interoperabilität klarer und präziser definieren.

Das Thema Interoperabilität an Schnittstellen des Smart Meter Gateways wird als sehr wichtig angesehen. Denn Interoperabilität schafft Investitionssicherheit und Planbarkeit für alle Stakeholder rund um das intelligente Messsystem.

Im Rahmen einer Interoperabilitätsanforderung erwarten wir

1) Eindeutigkeit des Standes der Technik: Das zentrale SMGW bekommt hier Optionsmöglichkeiten hinsichtlich zur Unterstützung unterschiedlicher Telegramm-Modi (T, C, S). Allerdings wird nur das Mode S als verpflichtend vorgesehen, wohingegen Mode C und T nur optional erwähnt werden. Zielführender wäre es, das Angebot der unterschiedlichen Modi auf SMGW Seite (stromversorgt) verpflichtend zu machen (muss Mode T und Mode C) und seitens der anzubindenden Systeme die Wahl (Energie, Funkdurchdringung, etc.) zu lassen Denn optionale Angebote auf Seiten des SMGW helfen wenig weiter, da ihre Umsetzung und soweit Nutzung über die anzubindenden Anlagen/Systeme nicht sicher gewählt werden kann.

2) Aktualität des Standes der Technik: Technische Spezifikationen sollten aktuell sein und nicht >10 Jahre alte Spezifikationen weiter fortführen („Wireless M-BUS: Anforderungen“). So verbleibt hier der veraltete ursprüngliche Telegramm-Modus weiterhin als „Muss“, obwohl durch OMS für weitere Entwicklungen nicht mehr empfohlen. D.h. zwischenzeitlich entwickelte oder noch zu entwickelnde anzubindende Systeme müssen in aktueller/zukünftiger Umsetzung einem heute bereits veralteten Modus folgen und ihre real umgesetzten, aktuell dem Stand der Technik entsprechenden Modi, werden ggf. nicht mehr unterstützt.

Zu 12.1. Einleitung

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

*Anmerkung: Dieses funktioniert nur, wenn am HAN nur ein SMGW installiert wurde.

Zu 13.1 Einordnung des Anwendungsfalls

Die aufgeführten Parameter beziehen sich auf SMGWs mit Mobilfunkmodems.
Ein TK-Management von n>1 SMGWs erfordert auch das Management von SMGWs mit Ethernet-Schnittstelle und benötigter Netzwerktechnik.

Zu 13.4 Zulässige Netzwerkdiagnosedaten

Die TK. Managementfunktionen müssen erweiterbar sein. Essentiell wichtig ist die Aufnahme der Bit Error Rate (BER) als vom Gerät ermittelte Größe mit negativem Exponent, sowie Latenzen (Round Trip Time).

Zu 13.7. Periodischer Versand

Zu der Bedingung...

Wenn der Konfigurationsparameter "Intervall periodisch" angegeben ist, MUSS das SMGW genau dieses Intervall verwenden. [REQ.NDS.Versand.60]

... stellt sich die Frage, wie das SMGW mit Diagnosemeldungen umgehen soll, wenn GWA oder EMT temporär nicht verfügbar sind. Das Verhindern von DDOS sollte sichergestellt werden durch geeignete Sammel- und Retry-Mechanismen.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 2.000 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.