Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Technische Richtlinie BSI TR-03109-5

Kommunikationsadapter

Version 1.0

Datum:2023-11-24, Commit:687ffe60

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

Inhalt

Abbildungsverzeichnis

1 Einleitung

1.1 Vorwort

Das Smart-Meter-Gateway (SMGW) mit integriertem Sicherheitsmodul bildet als sichere Kommunikationseinheit den Sicherheitsanker und funktionalen Kern eines jeden intelligenten Messsystems (iMSys). Es ist damit integraler Baustein bei der Digitalisierung der Energienetze und trägt durch seine Sicherheitsleistung und seinen breiten Funktionsumfang dazu bei, dass das zukünftige hochflexible Energienetz effektiv und effizient funktionieren kann. Hierzu soll das SMGW unter anderem die sichere Anbindung und Fernsteuerbarkeit von steuerbaren Einrichtungen am Netzanschlusspunkt ermöglichen. Die Wichtigkeit und Relevanz dieser Thematik, dass Cybersicherheit die Voraussetzung für eine erfolgreiche Digitalisierung der Energiewende und das SMGW der zentrale Sicherheitsanker ist, bekräftigt das neue [GNDEW]. Hierzu entwickelt das Bundesamt für Sicherheit in der Informationstechnik (BSI) neben den bereits verankerten Standards auch Vorgaben für das sichere und interoperable Steuern und Schalten weiter, um Datenschutz und Datensicherheit für diese wichtigen Smart-Grid-Anwendungsfälle zu gewährleisten.

Um die sichere kommunikative Anbindung von technischen Einrichtungen an das SMGW zu ermöglichen, hat das BSI die hier vorliegende TR entwickelt. *Kommunikationsadapter* eines SMGW sind an allen Schnittstellen des SMGW (WAN, LMN und HAN) denkbar. Mit dieser Technischen Richtlinie formuliert das BSI Mindestanforderungen an diejenigen Kommunikationsadapter im HAN, die eine sichere Anbindung von technischen Einrichtungen an das SMGW über dessen *TLS-Proxy-Funktion* ermöglichen (*CLS-Kommunikationsadapter*). Die Anforderungen sind für die technische Umsetzung maßgebend und beschreiben den Stand der Technik.

Durch die Umsetzung dieser Anforderungen können sowohl das Vertrauen in die Infrastruktur rund um das intelligente Messsystem gesteigert als auch die Risiken von Angriffen auf diese technischen Einrichtungen verringert werden. Damit einhergehend verlangen die gesetzlichen Anforderungen für die Digitalisierung der Energiewende aus dem novellierten Messstellenbetriebsgesetz (MsbG) in diesem Kontext:

Sofern nach § 19 Absatz 2 [MsbG] zur Datenverarbeitung energiewirtschaftlich relevanter Mess- und Steuerungsvorgänge ausschließlich solche technischen Systeme und Bestandteile eingesetzt werden dürfen, die den Anforderungen aus den §§ 21 und 22 MsbG genügen, enthält diese TR die technischen Anforderungen für eine sichere und interoperable Anbindung von technischen Einrichtungen – also innerhalb der Kundenanlage – an das SMGW, damit die energiewirtschaftlich relevanten Mess- und Steuerungsvorgänge rechtskonform abgewickelt werden können.

Damit können Messstellenbetreiber über das SMGW abrechnungs-, bilanzierungs- oder netzrelevante Standard- und Zusatzleistungen nach § 34 MsbG, insbesondere Standardleistungen nach § 34 Absatz 1 Nummer 1, 2, 4 und 5 MsbG sowie Zusatzleistungen nach § 34 Absatz 2 Satz 2 Nummer 2 bis 5 und 8, 9 und 11 MsbG, vollumfänglich abwickeln.

Zur Unterstützung der Umsetzung der technischen Mindestanforderungen an iMSys gemäß MsbG tragen Kommunikationsadapter bei, indem sich technische Einrichtungen mithilfe eines *CLS-Kommunikationsadapters* nach dieser TR an die HAN-Schnittstelle des SMGW sicher und interoperabel anbinden lassen. Für die Definition des CLS-Kommunikationsadapters sei auf ▸Abschnitt 2.1 verwiesen.

1.2 Präambel

Das Verfahren nach § 27 MsbG zur Erstellung und Veröffentlichung neuer Technischer Richtlinien des BSI wurde eingehalten. Das Einvernehmen mit der Physikalisch-Technischen Bundesanstalt (PTB) und der Bundesnetzagentur (BNetzA) wurde unter Anhörung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) hergestellt. Der Ausschuss Gateway-Standardisierung wurde in der Sitzung vom 5. Dezember 2023 zur BSI TR-03109-5 angehört. Der Zeitpunkt des Inkrafttretens wurde bekannt gemacht. Das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) hat der BSI TR-03109-5 zugestimmt.

1.3 Zielsetzung

In dieser Technischen Richtlinie werden zum einen funktionale Mindestanforderungen an CLS-Kommunikationsadapter gestellt, um eine vertrauliche und interoperable Kommunikation zwischen dem CLS-Kommunikationsadapter und dem SMGW zu gewährleisten. Durch den erfolgreichen Konformitätsnachweis wird das Vertrauen in die kommunikative Anbindbarkeit an das SMGW erhöht. Zudem wird im Sinne der Nach-

haltigkeit das interoperable Verhalten von CLS-Kommunikationsadaptern an der Schnittstelle zum *HAN des SMGW* gesteigert.

Zum anderen wird das Sicherheitsproblem für CLS-Komponenten, welche einen CLS-Kommunikationsadapter realisieren, definiert und IT-Sicherheitsanforderungen an diese gestellt. Das Vertrauen in diese CLS-Komponenten wird dahingehend gesteigert, dass sie die Annahmen an eine sichere Einsatzumgebung aus [PP-0073] angemessen erfüllen werden.

Mit "TR" wird im Folgenden die vorliegende BSI TR-03109-5 bezeichnet, sofern nicht explizit eine andere TR referenziert wird.

1.4 Zielgruppe

Die TR richtet sich an Hersteller von CLS-Komponenten, also von Geräten im *HAN des SMGW*, die einen CLS-Kommunikationsadapter realisieren.

1.5 Anwendungsbereich der TR

Mit dieser TR formuliert das BSI Mindestanforderungen an *CLS-Kommunikationsadapter*, die den *TLS-Proxy-Kanal* des SMGW nutzen und ihn HAN-seitig terminieren. Für die präzise technische Beschreibung zur Konkretisierung des Anwendungsbereichs sei auf ▸Abschnitt 2.1 bis ▸Abschnitt 2.5 verwiesen.

1.6 Inkrafttreten der TR-03109-5

Die Anforderungen der BSI TR-03109-5 zur sicheren Anbindbarkeit von CLS-Komponenten an das Smart-Meter-Gateway treten zum 1. Januar 2024 in Kraft. Der Nachweis zur Erfüllung der Anforderungen der BSI TR-03109-5 und der Einhaltung des Stands der Technik nach § 22 Absatz 2 MsbG

1. erfolgt grundsätzlich durch eine Zertifizierung des Bundesamtes für Sicherheit in der Informationstechnik,
2. kann für den Einbau im agilen Rollout nach § 31 Absatz 1 Nummer 2 MsbG ab dem 1. Januar bis zum 31. Dezember 2024 auch durch eine Herstellerselbsterklärung gemäß dem Muster [Herstellererklärung] erfolgen,
3. gilt für vor dem 1. Januar 2024 erfolgte Einbauten als erbracht, wenn die Anbindung an das Smart-Meter-Gateway den bis dahin geltenden Anforderungen, insbesondere dem in [PP-0073] und [TR-03109-1] niedergelegten Stand der Technik, entspricht.

Hersteller können Zertifizierungsanträge nach Nummer 1 ab dem Zeitpunkt der Veröffentlichung der BSI-TR-03109-5 beim BSI stellen.

1.7 Zertifizierungen

Die TR bildet die Grundlage für ein TR-Zertifizierungsverfahren gemäß [TR-Produkte], durch das die Interoperabilität eines CLS-Kommunikationsadapters zur Verwendung mit einem SMGW sowie die kommunikative Anbindung an das SMGW bestätigt werden muss.

Außerdem definiert die TR das passende Sicherheitsproblem und stellt entsprechende Sicherheitsziele und Mindestanforderungen an die Sicherheitsleistung der CLS-Komponente auf, die ein Hersteller einer CLS-Komponente durch eine IT-Sicherheitszertifizierung nachzuweisen hat. Zur Prüfung und zum Nachweis der IT-Sicherheitsleistungen wird die Beschleunigte Sicherheitszertifizierung (BSZ) des BSI angewendet (siehe [BSZ-Produkte]), wodurch angemessenes Vertrauen in die IT-Sicherheit generiert wird.

Es werden folgende Fälle nach Prüfung der Voraussetzungen (s. ▸Abschnitt 2.7.2) unterschieden: Zum einen die TR-Zertifizierung ohne BSZ und zum anderen die TR-Zertifizierung, die zusätzlich einen erfolgreichen Abschluss eines BSZ-Verfahrens erfordert.

Eine IT-Sicherheitszertifizierung nach BSZ ist nur dann notwendig, wenn dies für die CLS-Komponente nach ▸Abschnitt 2.9 festgestellt wurde (siehe ▸REQ.GEN.Schnittstellen.10).

1.8 Fachlich zuständige Stelle

Fachlich zuständig für die Fortentwicklung der TR ist das BSI.

Anschrift: Bundesamt für Sicherheit in der Informationstechnik
Referat DI 21 - Cybersicherheit für die Digitalisierung der Energiewirtschaft
Postfach 200363
53133 Bonn
E-Mail: SmartMeter@bsi.bund.de

Anmerkungen zur TR können an die o.a. Anschrift oder E-Mail-Adresse gerichtet werden.

1.9 Terminologie

Im Rahmen von Anforderungen und normativen Inhalten werden die in Großbuchstaben geschriebenen deutschen Schlüsselwörter auf Basis von [RFC2119] verwendet:

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

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

Begriff	Beschreibung
REQ	Requirement (dt. Anforderung). Beschreibt eine Anforderung an die Komponente und identifiziert sie mittels einer eindeutigen ID. Die Requirement-ID setzt sich zusammen aus der Kennzeichnung REQ, einer Abkürzung der fachlichen Einordnung (z.B. ITS für IT-Sicherheit), der Bezeichnung oder Kategorie (z.B. Schnittstellen) und einer in der Regel in Zehnerschritten fortlaufenden Nummer. Es werden Schlüsselwörter auf Basis von [RFC2119] verwendet.
ICS	Implementation Conformance Statement (dt. Konformitätserklärung zur Implementierung). Ein ICS definiert, welche zusätzlichen Informationen der Hersteller über die Komponente im Rahmen einer Produktzertifizierung deklarieren muss. Die Beschreibung des Herstellers zum ICS dient der Prüfstelle zum produktspezifischen Testen einer zugeordneten Anforderung. Über ein ICS kann beispielsweise angegeben werden, ob der Hersteller eine bestimmte SOLL-Anforderung erfüllt oder nicht. Ein ICS verfügt ebenso wie ein Requirement über eine eindeutige ID, welche sich analog zusammensetzt (mit der Kennzeichnung ICS).

Tabelle 1.1 Anforderungstypen

1.10 Aufbau der TR-03109-5

Die TR gliedert sich in die folgenden Kapitel:

In diesem ▸Kapitel 1 wird im wesentlichen der Anwendungsbereich, das Inkrafttreten, die Zielsetzung und die Zielgruppe des Dokumentes beschrieben.

In ▸Kapitel 2 werden die präzisen technischen Beschreibungen zur Konkretisierung des Anwendungsbereichs angeführt und die funktionalen Aspekte von CLS-Kommunikationsadaptern erläutert. Zudem werden die Akteure benannt, die in verschiedenen Rollen mit dem CLS-Kommunikationsadapter interagieren können.

▸Kapitel 3 beschreibt in Form von Fachlichen Anwendungsfällen (FA) Mindestfunktionalitäten an CLS-Kommunikationsadapter auf semantischer Ebene. Die Interoperabilität bei der Kommunikation mit dem SMGW wird darüber hinaus über Kommunikationsszenarien beschrieben.

- Kapitel 4 beschreibt anhand dieser Kommunikationsszenarien Anforderungen hinsichtlich der Kommunikation an der HAN-Schnittstelle des SMGW und der dort verwendeten Kommunikationsverbindungen und Protokolle.
- Kapitel 5 formuliert Anforderungen an die IT-Sicherheit von CLS-Komponenten. Dabei wird insbesondere das betrachtete Sicherheitsproblem beschrieben.
- Kapitel 6 enthält schließlich weitere funktionale und nicht-funktionale Anforderungen, die CLS-Kommunikationsadapter und CLS-Komponenten erfüllen müssen.

2 Technische Einleitung

2.1 Kommunikationsadapter des SMGW

Das SMGW verbindet die Netzwerke Wide Area Network (WAN), Local Metrological Network (LMN) und Home Area Network (HAN) miteinander, siehe [PP-0073] und [TR-03109], und weist separate, physisch getrennte Schnittstellen für diese Netzwerke auf, siehe ▸Abbildung 2.1. *Kommunikationsadapter* eines SMGW unterstützen die einheitliche und sichere kommunikative Anbindung an das SMGW und sind an all diesen Schnittstellen denkbar. Kommunikationsadapter sind logische Einheiten, die in physischen Komponenten realisiert sind.

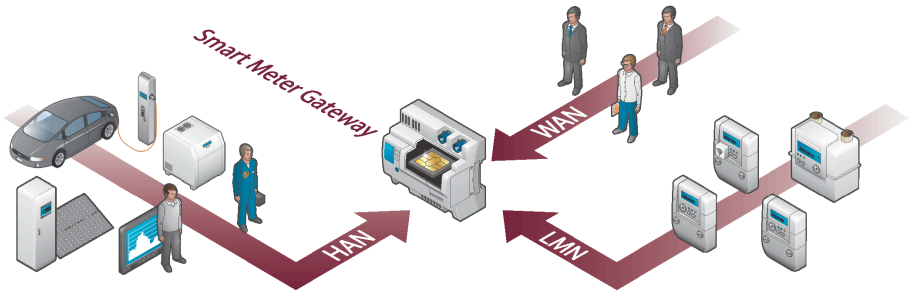

Abbildung 2.1. Systemarchitektur des intelligenten Messsystems (iMSys)

An der HAN-Schnittstelle des SMGW können steuerbare Einrichtungen wie beispielsweise Wärmepumpen, Wechselrichter von Photovoltaikanlagen oder Datenkonzentratoren angeschlossen werden, um externen Marktteilnehmern den Zugriff für Steuerungszwecke oder für Mehrwertdienste zu ermöglichen. Das SMGW stellt hierfür einen sicheren, transparenten Kanal zur Verfügung. Hierzu bietet das SMGW an der HAN-Schnittstelle über die logische Schnittstelle *IF_GW_CLS* die *TLS-Proxy-Funktion* an. Diese dient dem Aufbau und der Nutzung eines *TLS-Proxy-Kanals*, eines vom SMGW vermittelten, TLS-gesicherten Kommunikationskanals, der zwischen einer *CLS-Komponente* und einem *Kommunikationspartner im WAN* des SMGW etabliert wird.

Als *CLS-Kommunikationsadapter* werden diejenigen Kommunikationsadapter bezeichnet, die an die logische Schnittstelle IF_GW_CLS des SMGW angebunden werden, um den TLS-Proxy-Kanal des SMGW zu nutzen und insbesondere den vom SMGW bereitgestellten TLS-Proxy-Kanal HAN-seitig zu terminieren, siehe auch ▸Abbildung 2.2. CLS-Komponenten bezeichnen Komponenten im HAN des SMGW, die den CLS-Kommunikationsadapter realisieren, d.h. der CLS-Kommunikationsadapter ist immer Teil einer CLS-Komponente. Logische CLS-Kommunikationsadapter sind also in physischen CLS-Komponenten realisiert.

Die vorliegende TR beschreibt ausschließlich Mindestanforderungen an CLS-Kommunikationsadapter.

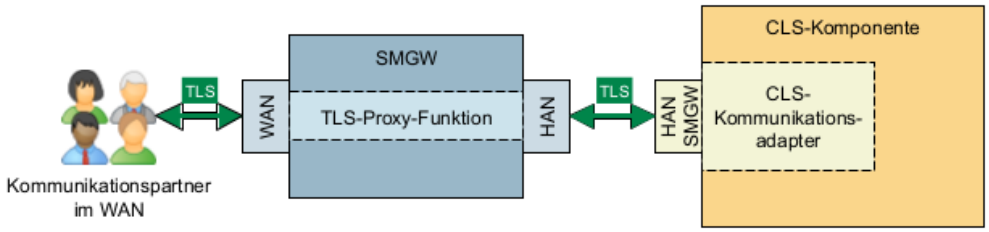

Abbildung 2.2. Nutzung der TLS-Proxy-Funktion des SMGW durch CLS-Kommunikationsadapter und CLS-Komponente. Pfeilkonturen deuten Verkabelungen an, grüne Pfeile stehen hier für eine TLS-Verbindung.

Die Mindestanforderungen dieser TR beziehen sich zum einen auf Interoperabilitätsanforderungen hinsichtlich der Kommunikation mit dem SMGW, der Nutzung dessen TLS-Proxy-Kanals, der Durchführung von Firmware-Updates und des Führens einer Systemzeit. Wenn für die CLS-Komponente nach ▸Abschnitt 2.9 festgestellt wurde, dass eine IT-Sicherheitszertifizierung nach BSZ notwendig ist (siehe ▸REQ.GEN.Schnittstellen.10), müssen zum anderen auch die Anforderungen an die IT-Sicherheit erfüllt werden

2.2 Systemarchitektur für CLS-Kommunikationsadapter

CLS-Kommunikationsadapter dienen dazu, *technische Einrichtungen* an die Schnittstelle IF_GW_CLS des SMGW anzubinden. Technische Einrichtungen sind unter anderem fernsteuerbare Verbrauchs- und Erzeugungsreinrichtungen gemäß [MsbG], [EEG], [EnWG], Steuerungseinrichtungen und Datenkonzentratoren für Mehrwertdienste.

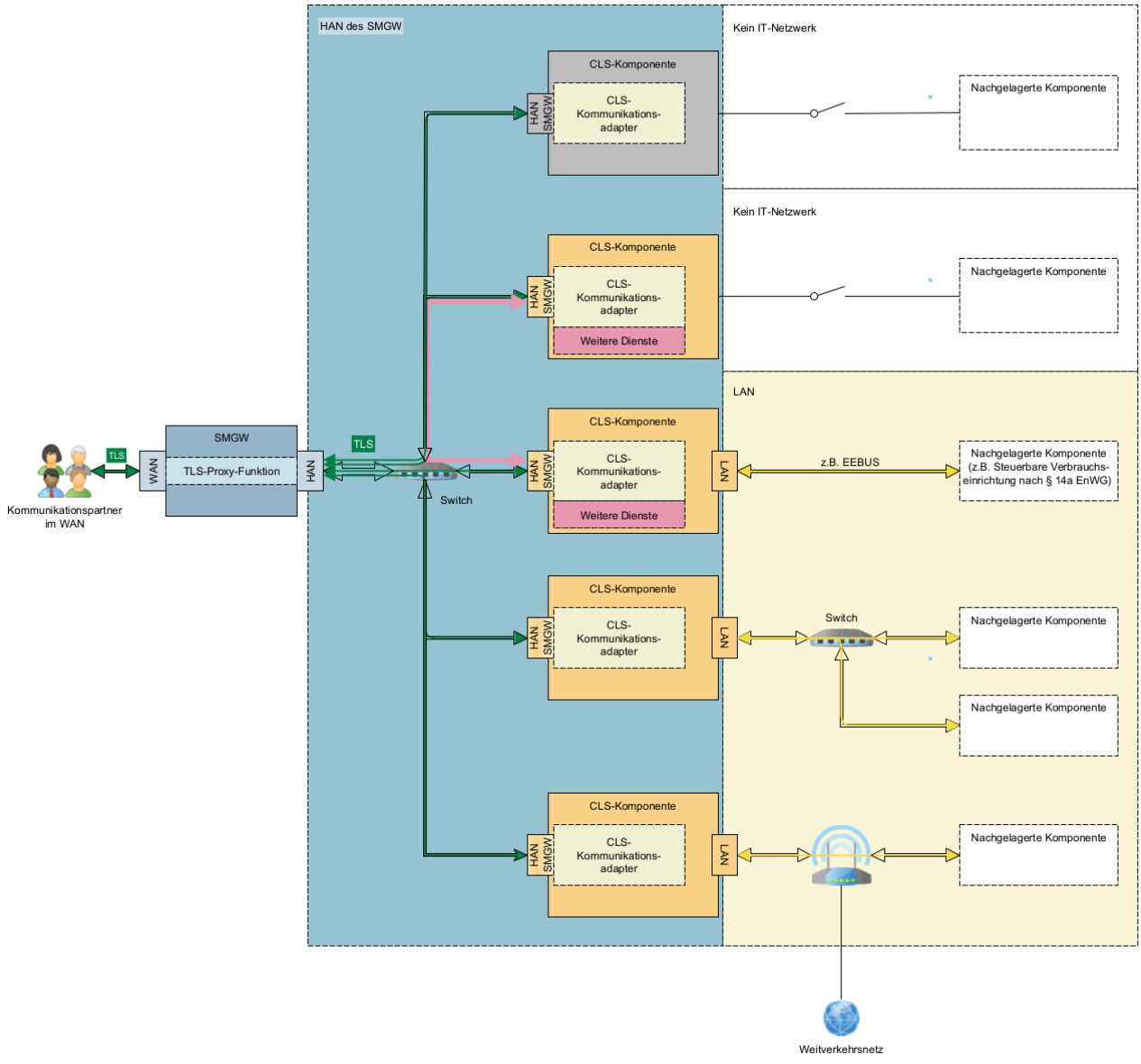

Abbildung 2.3. Beispiel für eine HAN-Systemarchitektur. Von oben nach unten: 1) CLS-Komponente ohne Einbindung in weitere Netze und ohne weitere Dienste im HAN des SMGW zu nutzen oder anzubieten, TR-Zertifizierung nötig; 2) CLS-Komponente ohne Einbindung in weitere Netze, aber weitere Dienste im HAN des SMGW werden genutzt oder angeboten (roter Pfeil), TR- und BSZ-Zertifizierung nötig; 3)-5) CLS-Komponente mit Einbindung in weitere Netze, TR- und BSZ-Zertifizierung nötig. Pfeilkonturen deuten physische Verbindungen (z.B. Verkabelungen) an, farbige Verbindungen stehen für TLS (grün), Dienste (rot) im *HAN des SMGW* (blauer Hintergrund) oder Dienste im LAN (gelb); Weitere Netze, z.B. das Anlagen- oder Kunden-LAN, ist hellgelb hinterlegt.

Über den CLS-Kommunikationsadapter sollen u.a. die verpflichtenden Zusatzdienstleistungen gemäß § 34 Absatz 2 MsbG und weitere optionale Mehrwertdienste durch die Nutzung des CLS-Kanals des SMGW ermöglicht werden. Aus diesem Grund ist es erforderlich, dass ein CLS-Backend-System mit mehreren CLS-Kommu-

nikationsadaptern, die unterschiedliche energiewirtschaftliche Anwendungsfälle abdecken, über verschiedene Anwendungsprotokolle kommunizieren kann. Beispiele hierfür sind derzeit genutzte Anwendungsprotokolle wie IEC 61850, CLS.EEDI (EEBUS) oder OpenADR.

Im Kontext dieser TR kann eine technische Einrichtung zum einen selbst die (physische) CLS-Komponente sein, die einen CLS-Kommunikationsadapter realisiert und die sich somit im HAN des SMGW befindet. Zum anderen kann eine technische Einrichtung eine *nachgelagerte Komponente* sein. Eine nachgelagerte Komponente ist ein physisches Gerät, das sich selbst nicht im HAN des SMGW befindet, aber physisch an eine CLS-Komponente angebunden ist. An eine CLS-Komponente können eine oder mehrere nachgelagerte Komponenten angebunden sein.[1]

Der Zertifizierungsumfang, siehe auch ▸Abschnitt 1.7 und ▸Abschnitt 2.4, richtet sich nach den verfügbaren Schnittstellen und Diensten der CLS-Komponente. Beispielhaft wird das in ▸Abbildung 2.3 illustriert: CLS-Komponenten und nachgelagerte Komponenten sind in unterschiedlichen Varianten abgebildet. Dabei ist der Teil der CLS-Komponente, an den sich die funktionalen Mindestanforderungen mit der zugehörigen TR-Zertifizierung richten, hellgrün gekennzeichnet. Die Zertifizierung nach BSZ betrachtet immer die gesamte CLS-Komponente (orange markiert zusammen mit hellgrün markiert).

Die Anforderungen an die Einsatzumgebung von SMGW gemäß [PP-0073] gelten weiterhin für alle Komponenten im HAN des SMGW.

2.3 Logische und physische Abgrenzung eines CLS-Kommunikationsadapters

2.3.1 Logische Abgrenzung

Der CLS-Kommunikationsadapter ist über die funktionalen Mindestanforderungen dieser TR definiert. Er nutzt den sicheren Kommunikationskanal des SMGW, d.h. dessen *TLS-Proxy-Funktion* und ist der TLS-Endpunkt dieses TLS-Proxy-Kanals im HAN des SMGW. Ein CLS-Kommunikationsadapter ist daher für die korrekte kommunikative Anbindung an das SMGW sowie die korrekte Verwendung des TLS-Proxy-Kanals – insbesondere die eventuelle Initiierung der TLS-Verbindung und das Aufrechterhalten des TLS-Proxy-Kanals – verantwortlich.[2] Zudem enthält jeder CLS-Kommunikationsadapter Funktionen für ein Firmware-Update, zum Führen einer Systemzeit und zur Konfiguration.

Ein CLS-Kommunikationsadapter besitzt mindestens eine logische Schnittstelle zum HAN des SMGW zur Nutzung der *TLS-Proxy-Funktion* des SMGW und in der Regel weitere logische Schnittstellen zur Kommunikation innerhalb der CLS-Komponente oder mit weiteren, an diese angeschlossenen, nachgelagerten Komponenten.

2.3.2 Physische Abgrenzung

Die physische Abgrenzung eines CLS-Kommunikationsadapters ist die CLS-Komponente, in der er realisiert ist. Diese CLS-Komponente befindet sich im HAN des SMGW und ist an die HAN-Schnittstelle des SMGW angebunden. Die physische Abgrenzung dieser CLS-Komponente ist die gesamte Hardware, die in ihrem Gehäuse integriert ist und die für die Bereitstellung der Funktionen gemäß ▸Abschnitt 2.3.1 benötigt wird. Die physische CLS-Komponente kann weitere Funktionalitäten außer den in dieser TR beschriebenen aufweisen. An diese Funktionalitäten oder deren Ausgestaltung werden nur Anforderungen bezüglich der IT-Sicherheit gestellt, siehe ▸Abschnitt 2.7.2 und ▸Kapitel 5.

Diese physische CLS-Komponente besitzt mindestens eine physische Schnittstelle zur Anbindung an die HAN-Schnittstelle des SMGW und gegebenenfalls weitere physische (oder logische) Schnittstellen zu anderen Komponenten im HAN des SMGW oder zu nachgelagerten Komponenten. [3]

---

[1] Über die Art der Anbindung trifft diese TR keine Aussage: So ist sowohl die kabellose, als auch die kabelgebundene Anbindung bis hin zur physischen Integration eines CLS-Kommunikationsadapters in eine nachgelagerte Komponente (z.B. als Hutschienengerät) denkbar.

[2] Der CLS-Kommunikationsadapter unterstützt somit die TLS-Proxy-Funktion gemäß [TR-03109].

[3] Diese TR trifft keine Aussage zur Möglichkeit, die physische Schnittstelle der CLS-Komponente für andere Dienste als den TLS-Proxy-Kanal zu nutzen.

2.4 Gegenstand der Konformitätsprüfung

Gegenstand der Konformitätsprüfung gemäß dieser TR ist die gesamte physische CLS-Komponente, die den CLS-Kommunikationsadapter realisiert.[4] Es wird geprüft, ob die CLS-Komponente die Funktionalitäts- und Interoperabilitätsanforderungen an ihren CLS-Kommunikationsadapter gemäß dieser TR erfüllt. Für den Fall, dass für die CLS-Komponente nach ▸Abschnitt 2.9 die Notwendigkeit einer IT-Sicherheitszertifizierung nach BSZ festgestellt wurde (siehe ▸REQ.GEN.Schnittstellen.10), wird innerhalb der Konformitätsprüfung außerdem geprüft, ob der Nachweis einer erfolgreichen IT-Sicherheitszertifizierung nach BSZ für diese CLS-Komponente vorliegt.

Beispielhaft sind in ▸Abbildung 2.3 CLS-Komponenten in orange zusammen mit hellgrün abgebildet, für die IT-Sicherheitszertifizierungen notwendig sind.

2.5 Mögliche Schnittstellen von CLS-Komponenten

Um sich mit dem SMGW zu verbinden, verfügt eine CLS-Komponente mindestens über eine physische und logische Schnittstelle zum HAN des SMGW.[5] Über diese logische Schnittstelle wird die TLS-Proxy-Funktion des SMGW genutzt und eine TLS-Verbindung zum SMGW aufgebaut beziehungsweise unterhalten.

Aufgrund der Heterogenität der möglichen CLS-Komponenten ist das Vorhandensein weiterer physischer und logischer Schnittstellen möglich. Von Relevanz ist im Folgenden die Unterscheidung zwischen den in ▸Tabelle 2.1 beschriebenen Kategorien von Schnittstellen.

Schnittstellenkategorie	Beschreibung
Schnittstelle zum HAN des SMGW	IT-Schnittstelle der CLS-Komponente, die zur Kommunikation mit dem SMGW für die HAN-Kommunikationsszenarien gemäß ▸Abschnitt 4.4 genutzt wird.
Fernzugriffsschnittstelle	*IT-Schnittstelle*, die für eine Kommunikation über ein *Weitverkehrsnetz*, z.B. das Internet, vorgesehen ist.
Lokale IT-Schnittstelle	*IT-Schnittstelle*, die nur für die lokale Kommunikation mit IT-Komponenten vorgesehen ist, technisch in der Lage ist Daten zu empfangen und nicht einer "Schnittstelle zum HAN des SMGW" entspricht. Darunter fallen physische Schnittstellen, wie beispielsweise Ethernet-, RS-485-, USB-, Powerline-, Fiber- oder Funkempfangs-Schnittstellen. Darunter fallen auch logische Schnittstellen von CLS-Komponenten. CLS-Komponenten, deren vorgesehener Verwendungszweck auch die netzorientierte Steuerung umfasst, können diese beispielsweise gemäß VDE-AR-E 2829-6 implementieren. Unabhängig von der vorgesehenen Verwendung kann es über eine solche Schnittstelle zu Fernzugriffen kommen, etwa bei unsachgemäßer Benutzung oder unbeabsichtigter Kopplung mit kompromittierten Geräten oder Netzwerken.
Weitere Schnittstelle	Schnittstelle, die keine der vorgenannten Eigenschaften erfüllt, etwa ein physischer Schalter oder ein Relais-Anschluss.

Tabelle 2.1 Schnittstellen von CLS-Komponenten

Da Interaktionen einer CLS-Komponente mit einem Weitverkehrsnetz zusätzliche Angriffsmöglichkeiten eröffnen, siehe ▸Abschnitt 2.7.2, sind Schnittstellen, die eine solche Interaktion grundsätzlich ermöglichen, auch für diese weitergehenden Angriffsmöglichkeiten als IT-sicherheitsrelevante Schnittstellen anzusehen und entsprechend abzusichern.

Die Informationen, die der Hersteller bezüglich der in der konkret betrachteten CLS-Komponente vorliegenden Schnittstellen deklarieren muss, sind in ▸Abschnitt 2.9 dargestellt.

Hinweis: Werden über die physische Schnittstelle, die zur Kommunikation mit dem SMGW vorgesehen ist, über die in ▸Abschnitt 4.4 verwendeten Ports und Protokolle hinaus Daten übertragen, handelt es sich um weitere lokale IT-Schnittstellen oder Fernzugriffsschnittstellen.

[4] Eine reine Software-Prüfung ist nicht möglich.

[5] Auch mehrere physische oder logische Schnittstellen zum HAN des SMGW sind möglich und zulässig.

Hinweis: Zur netzorientierten Steuerung nach § 14a EnWG und § 9 EEG finden sich Anwendungsfälle in der [VDE-AR-E 2829-6-1] und zur interoperablen Kommunikation zu nachgelagerten Komponenten in der [VDE-AR-E 2829-6-4] als mögliche Lösung für eine CLS-Komponente nach dieser TR.

2.6 Akteure

2.6.1 Übersicht über Akteure

Im Folgenden werden mögliche Akteure beschrieben, die mit der Funktionalität des CLS-Kommunikationsadapters interagieren können. Diese Liste ist aufgrund der Heterogenität der möglichen Ausprägungen von CLS-Kommunikationsadaptern und den CLS-Komponenten, in denen sie enthalten sind, nicht abschließend. Der CLS-Kommunikationsadapter selbst ist ebenfalls als Akteur anzusehen, wird aber nicht erneut aufgeführt.

Das Anwendungsfalldiagramm ▸Abbildung 2.4 verdeutlicht die Interaktion von Akteuren und CLS-Kommunikationsadapter im Rahmen der *Fachlichen Anwendungsfälle* (FA). Dabei ist zu beachten, dass hier nur FA-Kategorien abgebildet sind und dass Aussagen über die verpflichtende Umsetzung in ▸Abschnitt 2.8 zu finden sind.

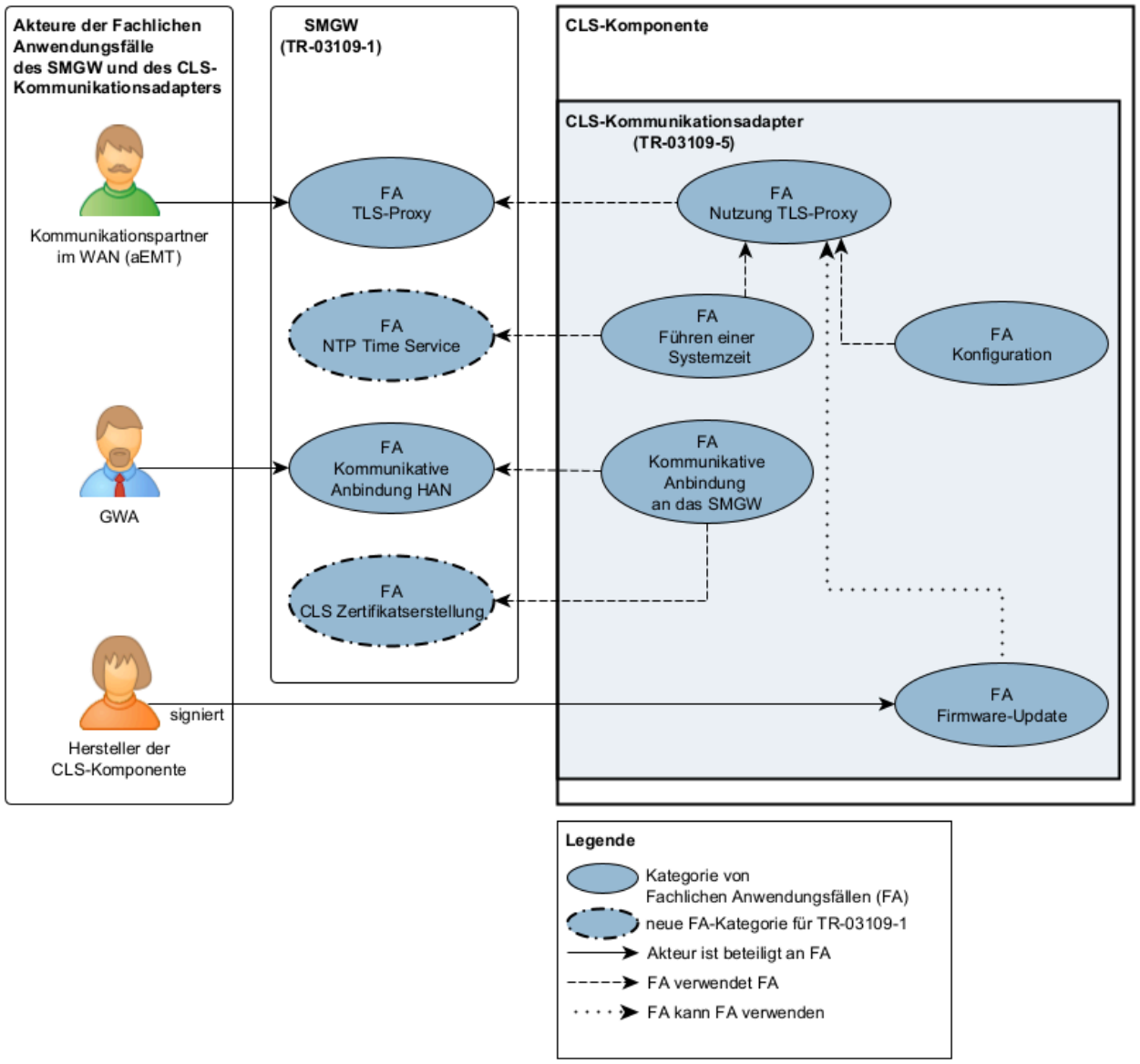

Abbildung 2.4. Interaktion von Akteuren und CLS-Kommunikationsadaptern im Rahmen der Fachlichen Anwendungsfälle. Gestrichelte FA-Kategorien des SMGW sind keine Mindestanforderungen der [TR-03109-1], aber für künftige Versionen der [TR-03109-1] vorgesehen.

Beziehungen zwischen FA werden durch gestrichelte Linien und Beziehungen zwischen Akteuren und FA durch durchgehende Linien dargestellt. Es ist zu beachten, dass in der Kategorie FA Firmware-Update nicht vorgegeben wird, über welche Schnittstelle oder durch welchen Akteur das Firmware-Update installiert wird, vgl. ▸Abschnitt 3.6.2. In dieser Abbildung wird ausschließlich die Beteiligung des Herstellers der CLS-Komponente am FA abgebildet, da dieser das Firmware-Update bereitstellt. Die Beteiligung weiterer Akteure am FA sowie die Verwendung der FA in der FA-Kategorie TLS-Proxy ist möglich, aber nicht vorgegeben, daher wird dies hier nicht abgebildet. Mit unterbrochenen Linien dargestellte FA des SMGW sind bis zur [TR-03109-1] Version 1.1 keine Mindestanforderungen, aber für künftige Versionen der [TR-03109-1] vorgesehen.

Informationen zum Konzept der FA und weitere Details zu den FA-Kategorien finden sich in ▸Abschnitt 3.1.

2.6.2 SMGW

Das SMGW ist als zentrale Kommunikationsplattform des iMSys mit Geräten in den Netzwerken WAN, LMN und HAN verbunden. Es ermöglicht CLS-Komponenten unter Verwendung der Funktionalität des CLS-Kommunikationsadapters zur Anbindung an seine IF_GW_CLS-Schnittstelle die Nutzung seiner TLS-Proxy-Funktion.

Die Mindestfunktionalität und Interoperabilitätsanforderungen an das SMGW sind in [TR-03109-1] und zugehöriger Detailspezifikation beschrieben. Die IT-Sicherheitsanforderungen an das SMGW und das Sicherheitsmodul des SMGW sind in [PP-0073] sowie [PP-0077] beschrieben.

2.6.3 Lokaler Nutzer

Der *lokale Nutzer* kann lokal mit CLS-Komponenten interagieren, entweder unmittelbar über eine lokale Schnittstelle der CLS-Komponente oder mittelbar über eine nachgelagerte Komponente. Er verwendet die Funktionalität des CLS-Kommunikationsadapters nur indirekt.

2.6.4 Hersteller

Der Hersteller produziert die CLS-Komponente und stellt Handbücher und Firmware-Updates dafür bereit.

2.6.5 GWA

Der Smart-Meter-Gateway-Administrator (GWA) ist verantwortlich für die Administration und Überwachung des SMGW sowie die kommunikative Anbindung der CLS-Komponenten an dessen IF_GW_CLS-Schnittstelle (unter Verwendung des CLS-Kommunikationsadapters). Darüber hinaus ist er auch für die Initiierung des TLS-Proxy-Kanals auf Anfrage eines berechtigten *aEMT* verantwortlich.

2.6.6 Kommunikationspartner im WAN

Der Kommunikationspartner im WAN beschreibt allgemein eine externe Entität im WAN des SMGW, mit der die CLS-Komponente unter Verwendung des CLS-Kommunikationsadapters über einen *TLS-Proxy-Kanal* kommunizieren kann. Der aEMT beispielsweise ist eine Ausprägung des Kommunikationspartners im WAN; eine mögliche Nutzung des CLS-Kommunikationsadapters für den aEMT ist das Einbringen von Steuerbefehlen.

2.6.7 Nachgelagerte Komponente

Eine nachgelagerte Komponente ist ein physisches Gerät oder System, das mit einer CLS-Komponente interagieren kann, sich aber selbst nicht im HAN des SMGW befindet. Beispiele für nachgelagerte Komponenten sind Wechselrichter von Photovoltaikanlagen.

2.7 Übersicht über die Anforderungen der TR

2.7.1 Anforderungen an die Funktionalität und Interoperabilität

In ▸Kapitel 3 und ▸Kapitel 4 werden die Anforderungen an die Funktionalität und Interoperabilität von CLS-Kommunikationsadaptern detailliert beschrieben.

2.7.2 Anforderungen an die IT-Sicherheit

Die Anforderungen an die IT-Sicherheit werden an die physische CLS-Komponente gestellt, die einen CLS-Kommunikationsadapter realisiert. Diese Anforderungen dienen der Abwehr von möglichen Angriffen auf die CLS-Komponente, auf ihre schützenswerten Güter und auf weitere Komponenten im HAN des SMGW. Dies beinhaltet auch Angriffe, die über angeschlossene nachgelagerte Komponenten geführt werden. Eine Erläuterung des Sicherheitsproblems findet sich in ▸Abschnitt 5.2.

Zur Prüfung des sicheren Firmware-Updates, des Schutzes der Komponenten im HAN des SMGW vor Angriffen aus Weitverkehrsnetzen sowie des Selbstschutzes wird die BSZ des BSI angewendet, siehe [BSZ-Produkte]. Das Schema der BSZ ist ein Produktzertifizierungsverfahren mit risikobasiertem Ansatz und bestätigt Sicherheitsaussagen über ein IT-Produkt in Form eines Zertifikats. Durch belastbare Zeit- und Kostenplanung können Aufwände für Hersteller gering gehalten und gleichzeitig ein hohes Vertrauensniveau in die Sicherheitsleistung des Produkts erzeugt werden.

Diese TR definiert für die BSZ die Parameter in Form eines Sicherheitsproblems, das insbesondere die beteiligten Akteure (User), Annahmen (Assumptions) an die Einsatzumgebung, die schützenswerten Güter (Assets) mit jeweiligem Schutzbedarf sowie die betrachteten Angreifer (wie etwa lokaler physischer Angreifer oder Weitverkehrsnetzangreifer) und Bedrohungen umfasst. Zudem werden Mindestanforderungen an die Sicherheitsfunktionalität von CLS-Komponenten formuliert, siehe ▸Abschnitt 5.3. Die Umsetzung der Sicherheitsaussagen gemäß diesem Sicherheitsproblem sowie die Umsetzung der Mindestanforderungen an die Sicherheitsfunktionalität kann im Rahmen der BSZ bestätigt werden. Eine IT-Sicherheitszertifizierung nach BSZ ist nur dann notwendig, wenn dies für die CLS-Komponente nach ▸Abschnitt 2.9 festgestellt wurde (siehe ▸REQ.GEN.Schnittstellen.10).

2.7.3 Weitere Anforderungen

Zusätzliche Anforderungen an CLS-Kommunikationsadapter und die CLS-Komponenten, die sie realisieren, finden sich in ▸Kapitel 6. Dort finden sich Mindestanforderungen an die Dokumentation (siehe ▸Abschnitt 6.1) sowie an Aufschriften und Identifikationsmöglichkeiten (siehe ▸Abschnitt 6.2).

2.8 Umsetzung der Anforderungen

In ▸Abschnitt 3.1 sowie ▸Abschnitt 4.4.3 finden sich Übersichten darüber, welche FA und welche HAN-*Kommunikationsszenarien* (HKS) verpflichtend (**MUSS**) und optional (**SOLL**) umzusetzen sind.

Die IT-Sicherheitsanforderungen an CLS-Komponenten werden in ▸Kapitel 5 spezifiziert.

In ▸Kapitel 6 sind die weiteren Anforderungen als einzelne Requirements abgebildet.

2.9 Abgrenzung des Prüfgegenstands und der Schnittstellen

In diesem Abschnitt werden Informationen zu CLS-Kommunikationsadaptern und den sie realisierenden CLS-Komponenten aufgelistet, die der Hersteller in einem ICS deklarieren muss. Außerdem werden die Bedingungen, unter denen der Nachweis einer erfolgreichen BSZ für die CLS-Komponente notwendig ist, formuliert.

REQ.GEN.Schnittstellen.10

Sofern die CLS-Komponente gemäß ▸ICS.GEN.Schnittstellen.20 über *Lokale IT-Schnittstellen* oder *Fernzugriffsschnittstellen* verfügt, so **MUSS** die CLS-Komponente nach BSZ gemäß [BSZ-Produkte] im Geltungsbereich "Komponenten im HAN des SMGW" zertifiziert sein.

REQ.GEN.Schnittstellen.20

Sofern die CLS-Komponente gemäß ▸ICS.GEN.Schnittstellen.20 nicht über *Lokale IT-Schnittstellen* oder *Fernzugriffsschnittstellen* verfügt, **DARF** die CLS-Komponente **NICHT** über Netzwerk-Protokolle und TCP/UDP-Ports an der physischen Schnittstelle zum HAN des SMGW kommunizieren, die über ▸Abschnitt 4.4 hinausgehen.

ICS.GEN.TLSProxy.10

Der Hersteller **MUSS** im ICS deklarieren, ob der CLS-Kommunikationsadapter die TLS-Proxy-Funktion des SMGW verwendet und die zugehörige TLS-Verbindung terminiert.[6]

ICS.GEN.Schnittstellen.10

Der Hersteller **MUSS** im ICS alle physischen und logischen Schnittstellen der CLS-Komponente identifizieren und beschreiben, welche Protokolle und Dienste (z.B. Ports) für diese verwendet werden und welcher Kategorie aus ▸Tabelle 2.1 sie zugeordnet werden. Hier sind auch Debug-Schnittstellen aufzuführen sowie software-seitig deaktivierte Schnittstellen.

ICS.GEN.Schnittstellen.20

Der Hersteller **MUSS** im ICS deklarieren, ob die CLS-Komponente über *Lokale IT-Schnittstellen* oder *Fernzugriffsschnittstellen* verfügt.

ICS.GEN.Schnittstellen.30

Der Hersteller **MUSS** im ICS deklarieren, ob die CLS-Komponente an der physischen *Schnittstelle zum HAN des SMGW* über die in ▸Abschnitt 4.4 genannten Netzwerk-Protokolle und TCP/UDP-Ports hinaus über weitere Netzwerk-Protokolle oder TCP/UDP-Ports kommuniziert.

ICS.GEN.Dokumentation.10

Der Hersteller **MUSS** im ICS die der CLS-Komponente beiliegenden Dokumentationen und Handbücher angeben.

ICS.GEN.Akteure.10

Der Hersteller **MUSS** im ICS deklarieren, welche Akteure mit der CLS-Komponente interagieren.

[6] Dieses ICS dient der Bewertung der Anwendbarkeit der TR für das Produkt des Herstellers. Wenn der CLS-Kommunikationsadapter die TLS-Proxy-Funktion des SMGW nicht verwendet, so ist die aktuelle Version dieser TR nicht anwendbar.

3 Funktionalitäten

3.1 Fachanwendungsfälle und FA-Kategorien

In diesem Kapitel werden Anforderungen auf semantischer Ebene betrachtet und *Fachanwendungsfälle* (FA) formuliert. Dabei umfasst ein FA eine Funktionalität, die aufgrund interner oder externer *Ereignisse* von einem CLS-Kommunikationsadapter abgearbeitet wird. Diese Funktionalität wird im FA aus rein fachlicher Sicht beschrieben, Kommunikationsprotokoll- und syntaktische Details werden an dieser Stelle abstrahiert. Anforderungen an die Protokolle zur Kommunikation mit dem SMGW werden in *Kommunikationsszenarien* (KS) zusammengefasst.

In ▸Kapitel 4 werden die Anforderungen an die KS beschrieben. Dabei werden Vorgaben an die Protokolle und Datenstrukturen gestellt.

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

In ▸Abbildung 3.1 wird dieser Zusammenhang zwischen FA, KS und DS abgebildet: FA enthalten Anforderungen an die Funktionalität und Verweise auf KS, die die Anforderungen an die Protokollstandards für die Kommunikation mit dem SMGW konkretisieren. Das Kapitel 3 beschreibt die semantische Interoperabilität, das Kapitel 4 die technische Interoperabilität.

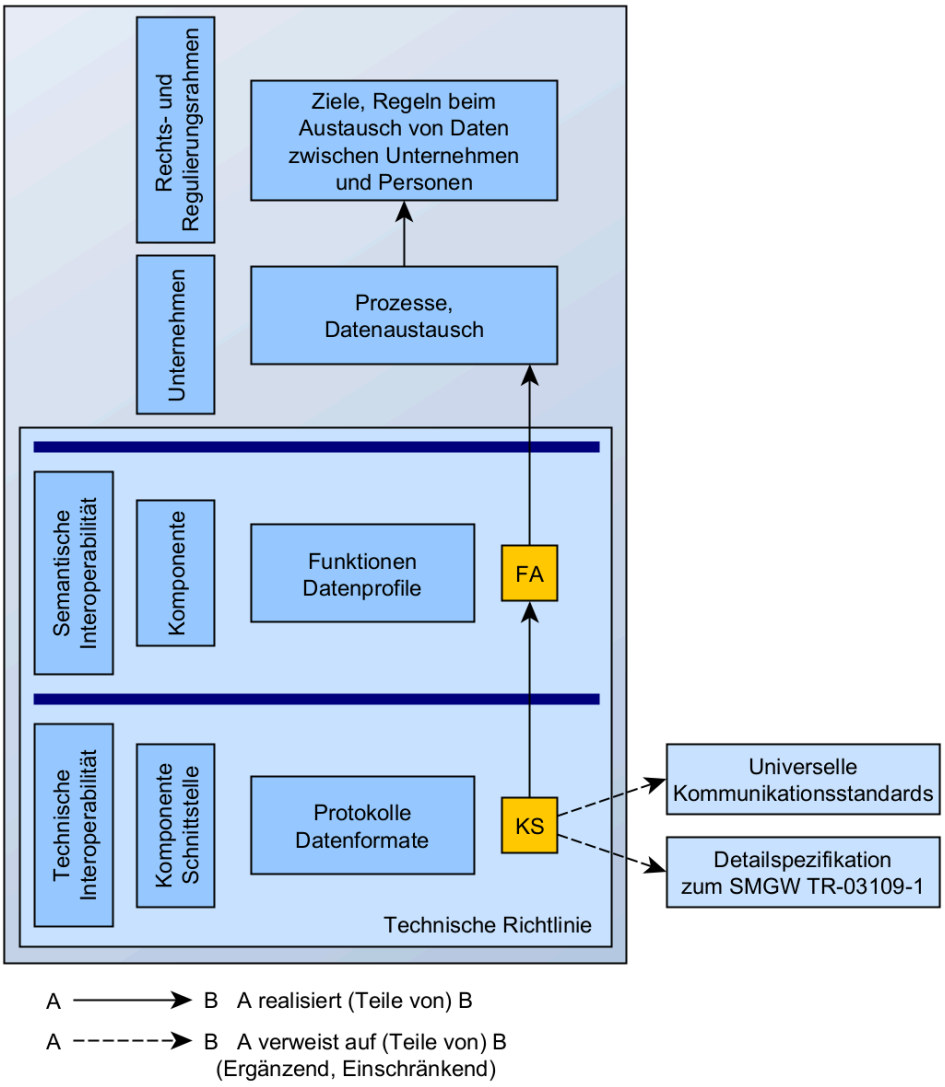

Abbildung 3.1. Interoperabilität-Modell der Technischen Richtlinie

Diese TR beschreibt für die kommunikative Anbindung und Zeitsynchronisation Anforderungen auf Anwendungsebene, nicht aber beispielsweise für Messwertübertragung oder Steuerung. Eine Interoperabilität bis zur Austauschbarkeit kann somit nur mit ergänzenden Anforderungsdokumenten erreicht werden, die produkt- oder fachspezifische Anforderungen an Semantik und Datenstrukturen der Anwendungsebene stellen.

FA-Kategorien sind Zusammenfassungen mehrerer FA, die fachlich zusammengehören. Leser, die sich einen Überblick über die Funktionen des CLS-Kommunikationsadapters verschaffen möchten, finden in der Übersicht der zugehörigen FA in der Einleitung der FA-Kategorie eine Zusammenfassung der Aufgaben der FA und können die detaillierte Beschreibung der FA überspringen.

Die Abschnitte der FA gliedern sich in folgende Unterabschnitte, die die Aufgabe, die Interaktion mit den Akteuren, Anforderungen an die Funktionalität und ggf. Implementierungshinweise beschreiben. Unterabschnitte sind nur bei Bedarf vorhanden.

Überschrift Die Überschrift eines Kapitels, in dem der FA beschrieben wird, ist eine eindeutige ID, um den FA leicht identifizieren und referenzieren zu können.

Beschreibung Die Beschreibung ist die textuelle Darlegung der Aufgabe des CLS-Kommunikationsadapters innerhalb des FA in Zusammenarbeit mit den Akteuren.

Auslöser Dieser Abschnitt beschreibt die Mindestanforderungen an Auslösebedingungen für den FA. Dazu gehören die auslösenden Akteure, sowie für externe Akteure die Kommunikationsszenarien bzw. Schnittstellen, über die die Auslösung stattfindet. Sofern notwendig, können auch ICS verankert sein, um für die Konformitätsbewertung notwendige Informationen vom Hersteller beschreiben zu lassen. Dies gilt unter anderem dann, wenn kein Kommunikationsszenario vorgegeben ist, aber Informationen bezüglich der Kommunikation für einen FA notwendig sind. Eine Übersicht möglicher Akteure ist in ▸Abschnitt 2.6 zu finden.

Anforderungen Dieser Abschnitt beinhaltet Anforderungen, wie der FA umzusetzen ist.

3.2 FA-Kategorie Kommunikative Anbindung an das SMGW

3.2.1 Einleitung

3.2.1.1 Voraussetzungen zur kommunikativen Anbindung

Bevor ein CLS-Kommunikationsadapter sicher mit einem SMGW kommunizieren kann, um die weiteren Fachanwendungsfälle auszuführen, muss die kommunikative Anbindung an das SMGW erfolgt sein. Die kommunikative Anbindung erfordert zunächst die Möglichkeit Nachrichten mit dem SMGW auszutauschen, nachdem CLS-Kommunikationsadapter und SMGW jeweils individuelle Netzwerkadressen im HAN erhalten haben (siehe ▸HKS.DNSDISCOVERY), um gesicherte Transportverbindungen zu vereinbarten Dienstadressen aufzubauen. Die Sicherung der Transportverbindungen erfolgt über Zertifikate, denen der jeweilige Kommunikationspartner vertraut. Dies können vom SMGW oder CLS-Kommunikationsadapter selbstsignierte Zertifikate oder ein SMGW Zertifikat aus der SM-PKI sein. Die Installation des *Vertrauensankers* zur Gewährleistung von Authentizität und Vertraulichkeit der Kommunikation mit dem SMGW erfolgt, unterstützt durch eine vertrauensvolle organisatorische Rolle (z.B. Hersteller, Installateur, Betreiber), vor der ersten Nutzung des SMGW-Zertifikates. Dies dient dem Schutz vor Man-in-the-Middle-Angriffen.

Die in den Fachanwendungsfällen zur Kommunikation mit dem SMGW verwendeten Kommunikationsszenarien geben eine beidseitige Authentifizierung der TLS-Verbindung vor.

3.2.1.2 Schlüsselpaar und Zertifikat des CLS-Kommunikationsadapters

Der CLS-Kommunikationsadapter besitzt zur TLS-Kommunikation mit dem SMGW ein Schlüsselpaar CLS_HAN_TLS_PRV/PUB und das Zertifikat CLS_HAN_TLS_CRT, das den öffentlichen Schlüssel CLS_HAN_TLS_PUB enthält und mit dem CLS_HAN_TLS_PRV signiert ist. Das Zertifikatsprofil ist in [DS] Kapitel HAN-Zertifikatsprofile beschrieben und entspricht CT_Selfsigned (Typ A) Funktion "cls".

Das Zertifikat enthält im *SubjectCN* eine Identifikation, die der Aufschrift auf der Komponente, die den CLS-Kommunikationsadapter enthält, entspricht (Siehe ▸Abschnitt 6.2).

Es wird empfohlen, die initialen CLS_HAN_TLS_PRV/PUB/CRT_0 bei der Herstellung im CLS-Kommunikationsadapter zu erzeugen (hier als **ClsKeyGen CLS** bezeichnet). Alternativ kann das initiale Schlüsselpaar und Zertifikat vom Hersteller erzeugt und ins CLS importiert werden (hier als **ClsKeyGen MFCT** bezeichnet).

Das initiale Zertifikat CLS_HAN_TLS_CRT_0 muss vom Hersteller (z.B. über digitale Begleitdokumente zur Lieferung) authentisch an den GWA des SMGW übermittelt werden, an den der CLS-Kommunikationsadapter kommunikativ angebunden werden kann. Der GWA konfiguriert dieses Zertifikat gemäß [TR-03109-1] im SMGW.[1]

Das SMGW stellt nur mit CLS-Kommunikationsadaptern eine Verbindung her, die zuvor im SMGW durch den GWA in einem Kommunikationsprofil hinterlegt und mit dem TLS-Zertifikat CLS_HAN_TLS_CRT konfiguriert wurden. Dieses Zertifikat dient der Berechtigungsprüfung und Authentifizierung des CLS-Kommunikationsadapters durch das SMGW.

Sobald Schlüsselpaar und Zertifikat des CLS-Kommunikationsadapters erneuert werden müssen, kann dies entweder im CLS-Kommunikationsadapter geschehen (**ClsKeyGen CLS**) oder durch Dienste des SMGW (**ClsKeyGen SMGW**).

Der private Schlüssel wird im Rahmen der IT-Sicherheitsanforderungen (Siehe ▸Kapitel 5) als Teil des schützenswerten Guts "Asset.Keys" modelliert. Er darf insbesondere nicht über eine Geräteschnittstelle zugänglich gemacht werden.

3.2.1.3 Authentifizierung des SMGW

Zur authentischen und vertraulichen TLS-Kommunikation zwischen SMGW und CLS-Kommunikationsadapter stellt das SMGW an der Schnittstelle IF_GW_CLS entweder sein Zertifikat aus der SM-PKI (für den **Pairing Mode PKI**) oder ein selbstsigniertes Zertifikat (für den **Pairing Mode DT**, direktes Vertrauen: Direct Trust) bereit. Entsprechend vertraut der CLS-Kommunikationsadapter entweder dem Aussteller dieses Zertifikates, d.h. einer Root- oder Sub-CA (**Pairing Mode PKI**), oder direkt einem SMGW-TLS-Zertifikat GW_HAN_TLS_CRT (**Pairing Mode DT**). **Pairing Mode PKI** ist dabei die zu bevorzugende Methode der Authentifizierung des SMGW.

Der CLS-Kommunikationsadapter besitzt einen Speicher für mehrere *Vertrauensanker* zur Validierung der im TLS-Handshake vom SMGW präsentierten Zertifikate. In diesem Speicher werden initial vom Hersteller des CLS-Kommunikationsadapters und die im Betrieb von Berechtigten importierten CA-Zertifikate oder Endnutzer-Zertifikate des SMGW integer und authentisch persistiert. [2]

SMGW-Zertifikate können also HAN-Zertifikate gemäß Detailspezifikation [DS] CT_Selfsigned (Typ A) oder CT_SMPKI_Signed (Typ C), nicht aber CT_CA_Signed (Typ B) sein. Für den Fall, dass das SMGW-Zertifikat CT_SMPKI_Signed verwendet wird, entspricht es dem GW_WAN_TLS_CRT.[3]

Die beiden Varianten, um das Vertrauen des CLS-Kommunikationsadapters in die Kommunikation mit einem SMGW herzustellen, sehen im Detail wie folgt aus:

- **Pairing Mode PKI**: Validierung mit CA-Vertrauensanker des GW_HAN_TLS_CRT

[1] In der Regel wird der Hersteller nicht direkt mit dem GWA kommunizieren, sondern es sind weitere Akteure wie der Kommunikationspartner im WAN daran beteiligt, das Zertifikat an den GWA zu übermitteln. Dies kann beispielsweise mittels elektronischen Lieferscheins geschehen. Diese Kommunikation wird hier verkürzt dargestellt.

[2] Die Variante **Pairing Mode DT** ist lediglich zur Anbindung von SMGW notwendig, die eine Authentifizierung gemäß **Pairing Mode PKI** noch nicht umsetzen können.

[3] Sofern der CLS-Kommunikationsadapter als TLS-Client eine Verbindung zum SMGW aufbaut, ignoriert er die in der Zertifikats-Extension "extended key usage" vorgegebene Restriktion auf "Webservice-Client" und nutzt das Zertifikat für die Authentifizierung des SMGW.

  - Während der Installation des CLS-Kommunikationsadapters wird gewährleistet, dass CLS-Kommunikationsadapter und zugeordnetes SMGW[4] im HAN miteinander kommunizieren.
  - Der CLS-Kommunikationsadapter wird ab Werk mit dem Root-CA-Zertifikat der SM-PKI ausgeliefert, mit dem er das im TLS-Handshake zur Authentifizierung des SMGW präsentierte GW_HAN_TLS_CRT bis zum *Vertrauensanker* validieren kann[5]. Es können Root- oder Sub-CA-Signatur-Zertifikate der SM-PKI (siehe [TR-03109-4]) als Vertrauensanker genutzt werden. In diesem Fall wird keinem individuellen SMGW vertraut, sondern einem zertifizierten SMGW als Gerätetyp.
  - Der CLS-Kommunikationsadapter muss im Falle eines CA-Vertrauensanker-Wechsels für das GW_HAN_TLS_CRT fähig sein, den neuen Vertrauensanker verwenden zu können (z.B. durch Link-Zertifikate, ein Firmware-Update, einen Download, oder als Konfiguration durch einen Kommunikationspartner im WAN), siehe ▸Abschnitt 3.2.1.4.
- **Pairing Mode DT**: "Pinning" des GW_HAN_TLS_CRT
  - Während der Installation des CLS-Kommunikationsadapters wird gewährleistet, dass CLS-Kommunikationsadapter und das ihm zugeordnete SMGW[6] im HAN miteinander kommunizieren.
  - Sobald der CLS-Kommunikationsadapter die technische Möglichkeit hat, das vom SMGW präsentierte GW_HAN_TLS_CRT zu validieren, muss er das SMGW authentifizieren.
  - Der CLS-Kommunikationsadapter wechselt in einen Zustand, in dem er das SMGW ausschließlich mit dem persistierten GW_HAN_TLS_CRT authentifiziert.
  - Vor einem anstehenden Wechsel des GW_HAN_TLS_CRT im SMGW durch den GWA wird im CLS-Kommunikationsadapter administrativ ein Zustand hergestellt, mit dem er das SMGW sowohl mit dem $GW\_HAN\_TLS\_CRT_n$ als auch einem neuen $GW\_HAN\_TLS\_CRT_{n+1}$ authentifiziert und nach erfolgreicher Authentifizierung dann persistiert, siehe ▸Abschnitt 3.2.1.4.

Da im CLS-Kommunikationsadapter bei einem CA-Zertifikatswechsel des GW_HAN_TLS_CRT zwei Vertrauensanker zur Validierung vorliegen, kann der CLS-Kommunikationsadapter dem SMGW im TLS-Handshake (je nach TLS-Version mittels Extension oder CertificateRequest "Certificate_Authorities") einen Hinweis auf die im CLS-Kommunikationsadapter vorliegenden CA-Zertifikate übermitteln (siehe [DS] Kapitel TLS), so dass das SMGW in der Überlappungsphase das geeignete GW_HAN_TLS_CRT im TLS-Handshake zur Authentifizierung verwendet.

Sofern nicht SMGW als auch CLS-Kommunikationsadapter die Vereinbarung von "Certificate_Authorities" unterstützen, kann durch Wiederholung des TLS-Handshakes mit dem bisherigen und künftigen GW_HAN_TLS_CRT bzw. dessen CA-Zertifikat ein TLS-Verbindungsaufbau zwischen SMGW und CLS durchgeführt werden.

▸Abbildung 3.2 zeigt die Interaktion von Hersteller, CLS-Kommunikationsadapter und GWA bei Erzeugung und Übermittlung der individuellen Informationen zur kommunikativen Anbindung an das SMGW.

[4] Gemäß [TR-03109-1] findet die Zuordnung über das CLS_HAN_TLS_CRT des Proxy-Kommunikationsprofiles statt.

[5] Das SMGW übermittelt auch das zugehörige SubCA-Zertifikat CA_SIG_CRT in der Zertifikatskette im TLS-Handshake.

[6] Gemäß [TR-03109-1] findet die Zuordnung über das CLS_HAN_TLS_CRT des Proxy-Kommunikationsprofiles statt.

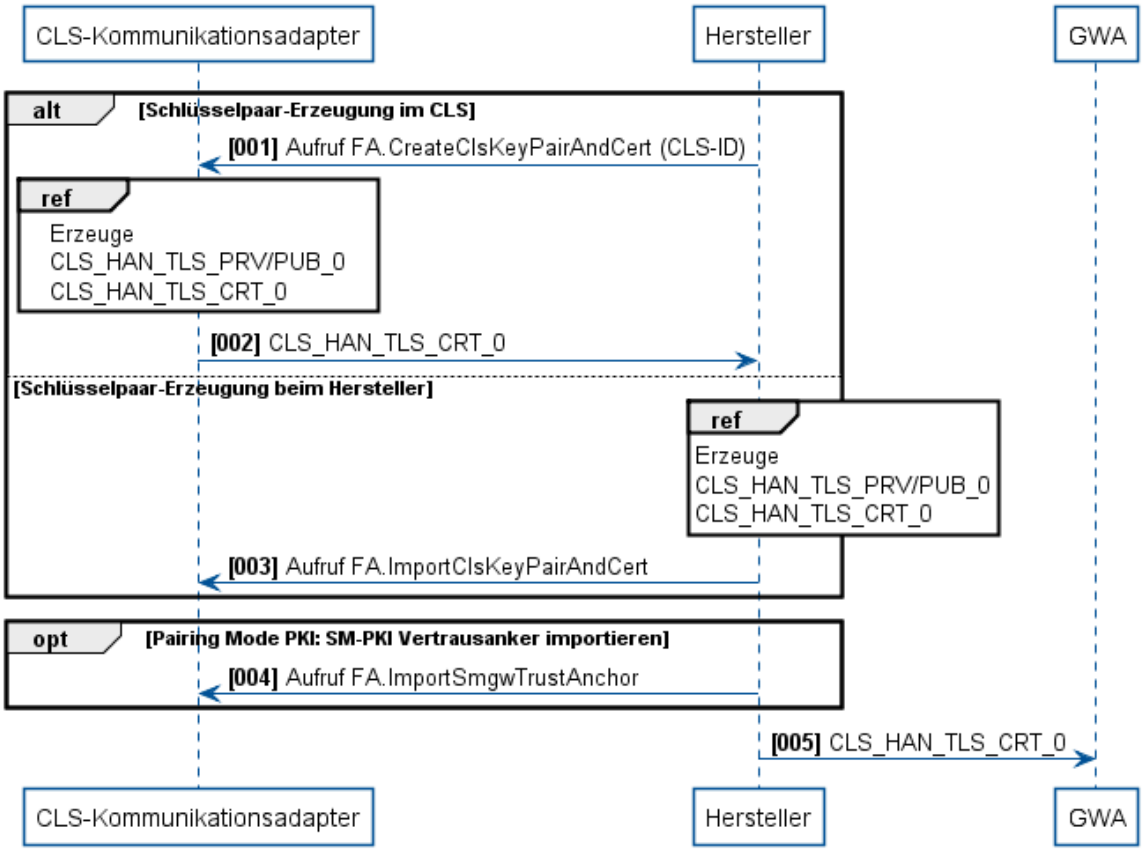

Abbildung 3.2. Erzeugung und Persistierung des kryptografischen Materials für TLS-Verbindungsaufbau im HAN des SMGW

Abbildung 3.3 zeigt die Interaktion von CLS-Kommunikationsadapter, GWA, SMGW bei der Installation.

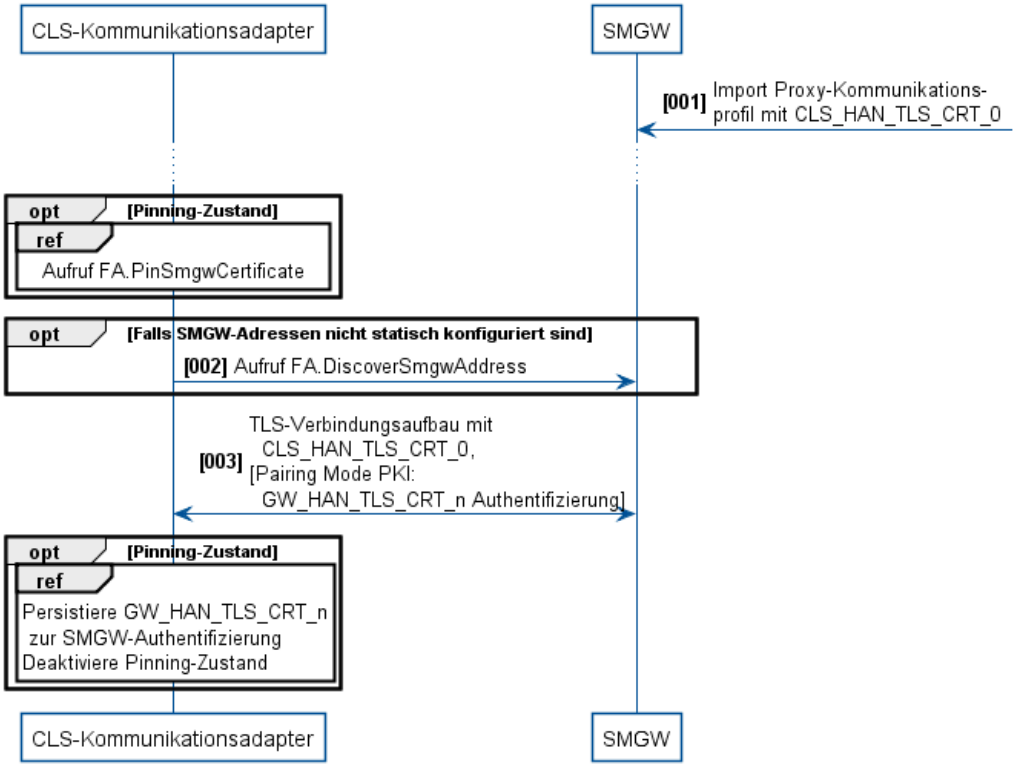

Abbildung 3.3. Installation des CLS-Kommunikationsadapters

3.2.1.4 Zertifikatswechsel

Der CLS-Kommunikationsadapter muss auf einen Zertifikatswechsel sowohl des SMGW-Zertifikates als auch des Zertifikates des CLS-Kommunikationsadapters selbst vorbereitet sein. Sofern das GW_HAN_TLS_CRT gewechselt wird, muss der CLS-Kommunikationsadapter in der Lage sein, dem neuen SMGW-Zertifikat zu vertrauen (Siehe ▸FA.ImportSmgwTrustAnchor oder ▸FA.PinSmgwCertificate).

Soll ein CLS-Kommunikationsadapter — z.B. nach Austausch eines SMGW — mit einem anderen SMGW kommunizieren, so muss die kommunikative Anbindung zum bisherigen SMGW aufgehoben (über ▸FA.DeactivateSmgwTrustAnchor oder ▸FA.RestoreDefaults) und zu einem neuen SMGW initial hergestellt werden.

Wechsel des TLS-Zertifikates des CLS-Kommunikationsadapters

▸Abbildung 3.4 zeigt den Ablauf der Interaktion mit dem CLS-Kommunikationsadapter beim Wechsel des CLS_HAN_TLS-Zertifikates.

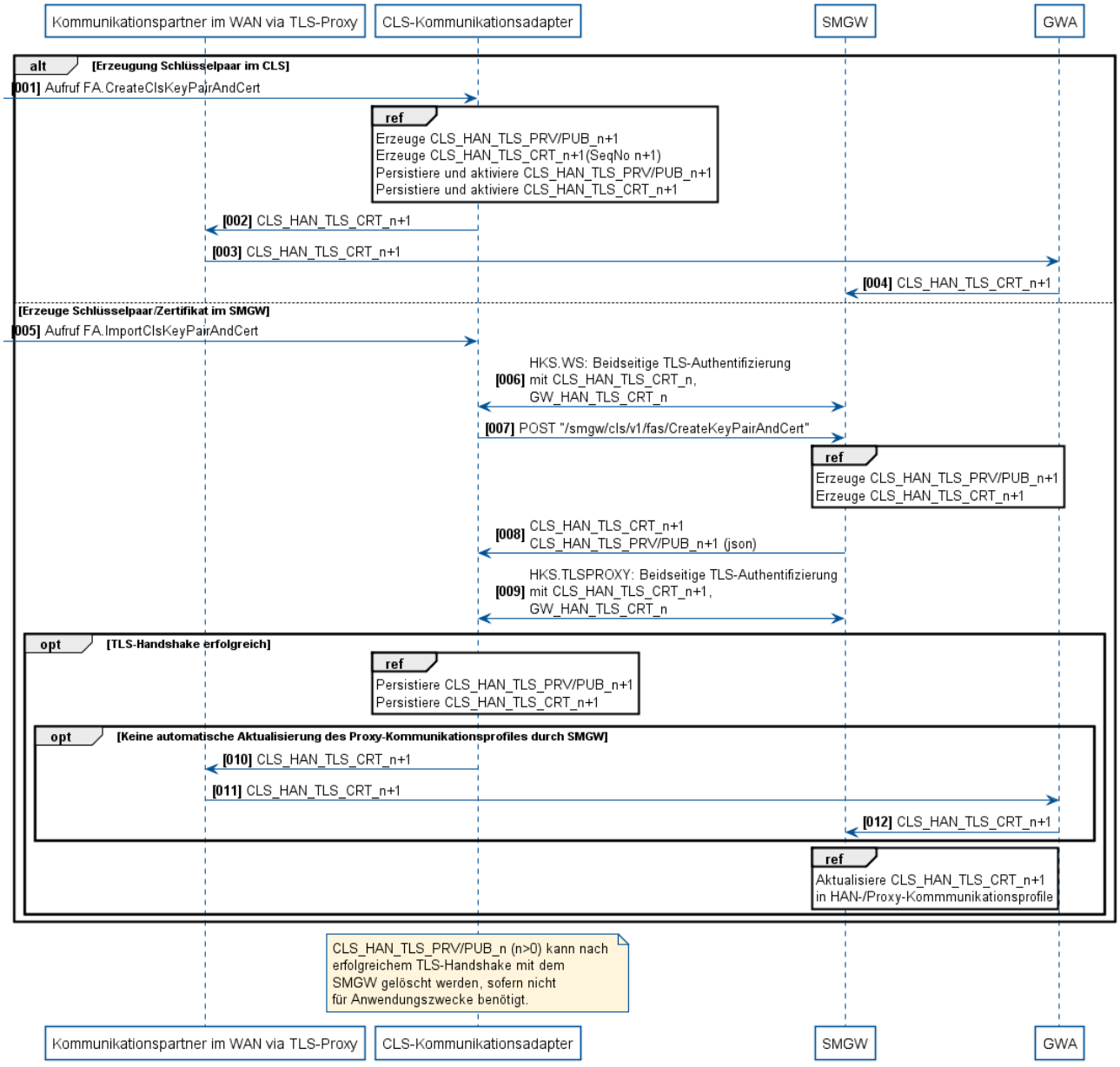

Abbildung 3.4. Zertifikatswechsel des CLS-Kommunikationsadapters

Wechsel des HAN-TLS-Zertifikates des SMGW

▸Abbildung 3.5 zeigt den Ablauf der Interaktion mit dem CLS-Kommunikationsadapter beim Wechsel des GW_HAN_TLS-Zertifikates.

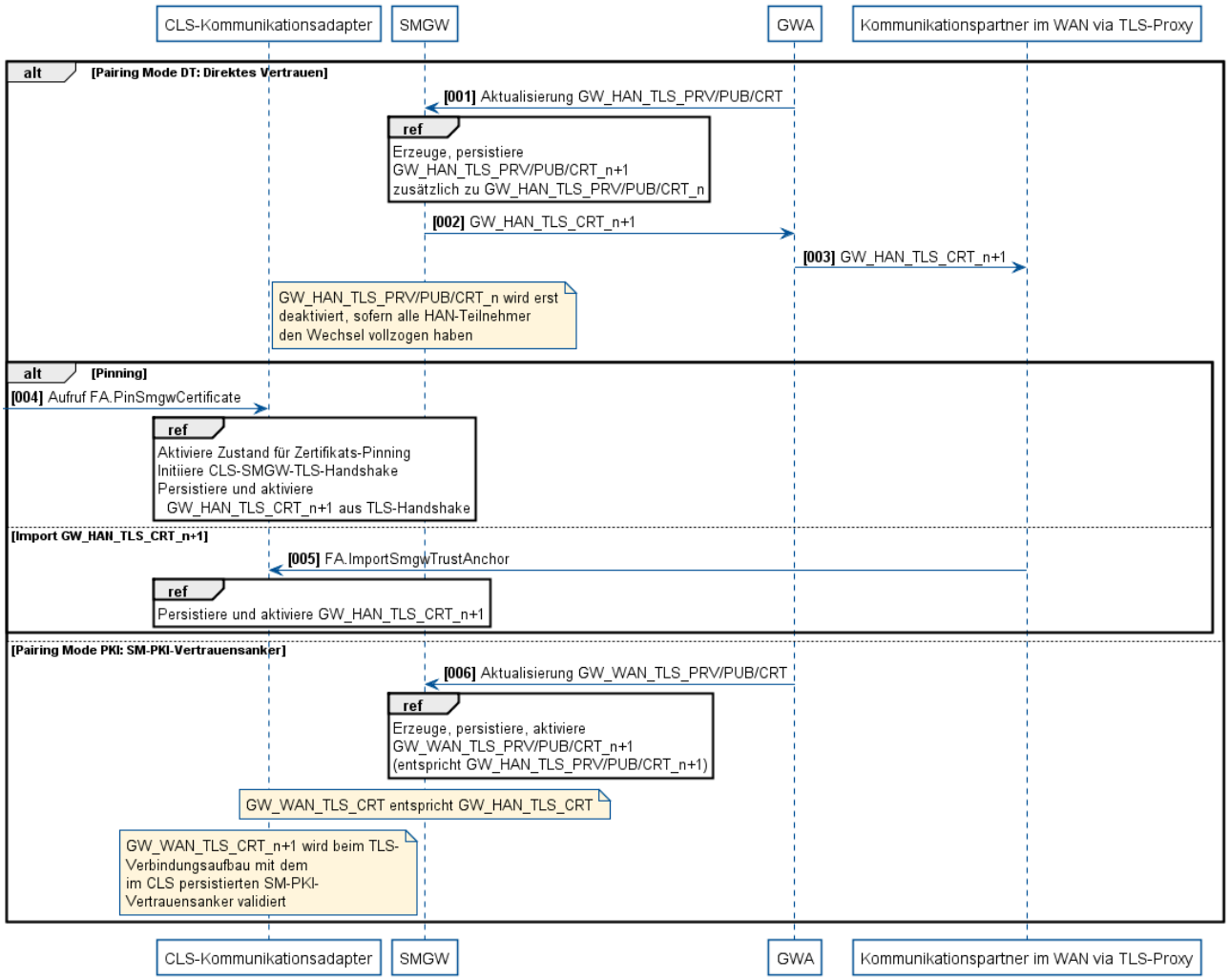

Abbildung 3.5. Zertifikatswechsel des SMGW-TLS-Zertifikates

Wechsel des (SM-PKI-)CA-Zertifikates für das HAN-TLS-Zertifikat des SMGW

▸Abbildung 3.6 zeigt den Ablauf der Interaktion mit dem CLS-Kommunikationsadapter beim Wechsel des GW_HAN_TLS-Vertrauensankers.

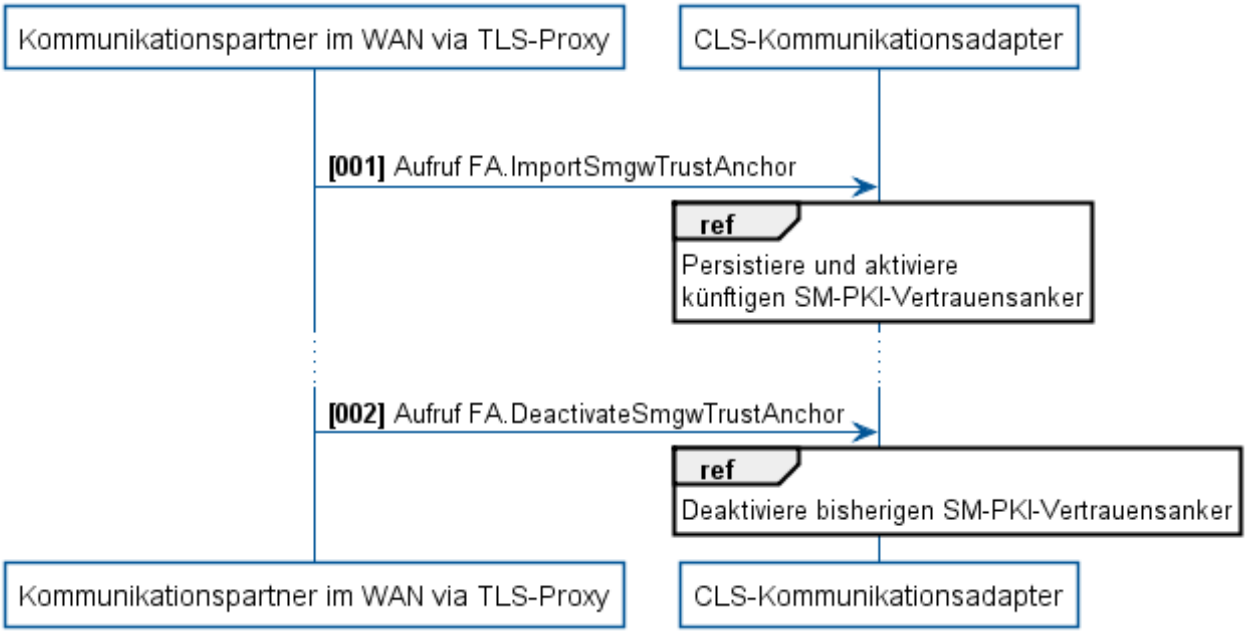

Abbildung 3.6. Zertifikatswechsel des Vertrauensankers für das SMGW-TLS-Zertifikat

Die folgende Tabelle enthält eine Übersicht darüber, wie die folgenden FA kombiniert werden können, um typische Aufgaben bei der kommunikativen Anbindung an ein SMGW zu erreichen.

Aufgabe	Umsetzung
Feststellen der SMGW-Adresse durch den CLS-Kommunikationsadapter	Der CLS-Kommunikationsadapter **MUSS** den ▸FA.DiscoverSmgwAddress implementieren, sofern der CLS-Kommunikationsadapter mindestens ein Kommunikationsszenario aus HKS.NTP-TLS.CLI, HKS.WS1.CLI, HKS.TLSPROXY.CLI oder HKS.TLSPROXY.SOCKSCLI implementiert. [REQ.FAKAT.SmgwAssociation.10]
Erzeugen eines Schlüsselpaares und Zertifikates durch den CLS-Kommunikationsadapter	Der CLS-Kommunikationsadapter **MUSS** den ▸FA.CreateClsKeyPairAndCert implementieren. [REQ.FAKAT.SmgwAssociation.70]
Import eines vom SMGW erzeugten Schlüsselpaares und Zertifikates des CLS-Kommunikationsadapters	Der CLS-Kommunikationsadapter **SOLL** den ▸FA.ImportClsKeyPairAndCert implementieren. [REQ.FAKAT.SmgwAssociation.60]
Kommunikative Anbindung des CLS-Kommunikationsadapters an ein SMGW mittels Zertifikats-Pinnings durch den TLS-Proxy-Kanal	Der CLS-Kommunikationsadapter **MUSS** den ▸FA.PinSmgwCertificate implementieren. [REQ.FAKAT.SmgwAssociation.20]
Kommunikative Anbindung des CLS-Kommunikationsadapters an ein SMGW mittels vorkonfigurierten Vertrauensankers	Der CLS-Kommunikationsadapter **MUSS** den ▸FA.ImportSmgwTrustAnchor bei der Erstkonfiguration implementieren. [REQ.FAKAT.SmgwAssociation.30]
Import eines Zertifikatsvertrauensankers des SMGW über den TLS-Proxy-Kanal	Der CLS-Kommunikationsadapter **MUSS** den ▸FA.ImportSmgwTrustAnchor für die Übermittlung des neuen Vertrauensankers über den TLS-Proxy-Kanal implementieren. [REQ.FAKAT.SmgwAssociation.40]
Deaktivieren des aktuellen Vertrauensankers im CLS-Kommunikationsadapter	Der CLS-Kommunikationsadapter **MUSS** den ▸FA.DeactivateSmgwTrustAnchor für die Deaktivierung eines SMGW-Vertrauensankers über den TLS-Proxy-Kanal implementieren. [REQ.FAKAT.SmgwAssociation.50]

Tabelle 3.1 Übersicht über die FA zur kommunikativen Anbindung an das SMGW

ICS.FA.ImportClsKeyPairAndCert.10

Der Hersteller **MUSS** im ICS deklarieren, ob der CLS-Kommunikationsadapter den ▸FA.ImportClsKeyPairAndCert vom SMGW unterstützt, sofern der FA zur Erzeugung von CLS_HAN_TLS_PRV/PUB/CRT gemäß [TR-03109-1] vom SMGW über ein HAN-Kommunikationsszenario spezifiziert ist.

3.2.2 FA.DiscoverSmgwAddress

3.2.2.1 Beschreibung

Dieser FA wird aufgerufen, um die Adresse(n) eines SMGW im HAN automatisiert zu bestimmen. Dieser FA dient zur Vereinfachung der Kontaktaufnahme eines CLS-Kommunikationsadapters zum SMGW, indem statt einer statischen Vereinbarung von Adressen vereinbarte Bezeichner ("smgw" oder herstellerübergreifende Identifikation des SMGW) verwendet werden, die in Adressen aufgelöst werden. Dazu gibt es folgende Möglichkeiten:

- Der CLS-Kommunikationsadapter ermittelt die Adresse(n) eines anhand der *SMGW-ID* identifizierten SMGW ("Unique Name").
- Der CLS-Kommunikationsadapter ermittelt die Adresse(n) eines SMGW ohne Kenntnis der *SMGW-ID* ("Shared Name").

Anschließend kann der CLS-Kommunikationsadapter sichere Transport-Verbindungen zum SMGW herstellen oder vom SMGW entgegennehmen.

Die ermittelten Netzwerk- und Dienstadressen können im CLS-Kommunikationsadapter für spätere Verwendung über einen Neustart hinaus persistiert werden oder bei Bedarf über diesen FA erneut ermittelt werden.

3.2.2.2 Auslöser

REQ.FA.DiscoverSmgwAddress.10

Sofern keine Netzwerkadresse im CLS-Kommunikationsadapter konfiguriert ist, **MUSS** der CLS-Kommunikationsadapter den FA bei folgenden Ereignissen auslösen:

- Innerhalb von 10 s nach Herstellen der Netzwerkverbindung ("Link") der Komponente und Erreichen der Betriebsbereitschaft

3.2.2.3 Anforderungen

Der CLS-Kommunikationsadapter **MUSS** die Bestimmung der SMGW-Adresse(n) über ▸HKS.DNSDISCOVERY durchführen und bis zur erneuten Adressbestimmung für die Kommunikation mit dem SMGW verwenden. [REQ.FA.DiscoverSmgwAddress.20]

3.2.3 FA.CreateClsKeyPairAndCert

3.2.3.1 Beschreibung

Dieser FA beschreibt die Erzeugung eines neuen Schlüsselpaares CLS_HAN_TLS_PRV/PUB$_{n+1}$ und des zugehörigen Zertifikates CLS_HAN_TLS_CRT$_{n+1}$ (Siehe [DS] Kapitel HAN-Zertifikatsprofile) vom CT_Selfsigned (Typ A), Funktion "cls" im CLS-Kommunikationsadapter, automatisiert durch den CLS-Kommunikationsadapter oder auf Veranlassung eines berechtigten externen Akteurs (in ▸Abschnitt 3.2.1.2 mit **ClsKeyGen CLS** bezeichnet).

Die Erzeugung des Schlüsselpaares im CLS-Kommunikationsadapter mit einem geeigneten Zufallszahlengenerator ([TR-03116-4] Kapitel 7) wird empfohlen. Der private Schlüssel wird im Rahmen der IT-Sicherheitsanforderungen (Siehe ▸Kapitel 5) als Teil des schützenswerten Guts "Asset.Keys" modelliert. Er darf insbesondere nicht über eine Geräteschnittstelle zugänglich gemacht werden. Es ist zu beachten, dass im Rahmen der IT-Sicherheitsanforderungen weitere Anforderungen an kryptographisches Material gestellt werden können.

3.2.3.2 Auslöser

REQ.FA.CreateClsKeyPairAndCert.10

Der CLS-Kommunikationsadapter **MUSS** den FA bei den in ▸ICS.FA.CreateClsKeyPairAndCert.10 beschriebenen Ereignissen auslösen.

ICS.FA.CreateClsKeyPairAndCert.10

Der Hersteller **MUSS** im ICS deklarieren, durch welche Ereignisse und Akteure der ▸FA.CreateClsKeyPairAndCert zur Erzeugung eines neuen Schlüsselpaares CLS_HAN_TLS_PRV/PUB und Zertifikates CLS_HAN_TLS_CRT ausgelöst wird (mindestens eines). Ein solches Ereignis kann dabei auch durch den CLS-Kommunikationsadapter selbst ausgelöst werden. Wird ein Ereignis durch einen Akteur ausgelöst, der nicht der CLS-Kommunikationsadapter selbst ist, so **MUSS** der Hersteller im ICS deklarieren, wie Akteur und CLS-Kommunikationsadapter miteinander kommunizieren und über welche Schnittstelle bzw. welches Kommunikationsszenario diese Kommunikation geschieht.

3.2.3.3 Anforderungen

Der CLS-Kommunikationsadapter **MUSS** ein Schlüsselpaar CLS_HAN_TLS_PUB/PRV$_{n+1}$ gemäß [TR-03109-3] und [TR-03116-4] für die Verwendung mit TLS im HAN erzeugen, speichern und im nächsten TLS-Handshake verwenden. [REQ.FA.CreateClsKeyPairAndCert.20]

Der CLS-Kommunikationsadapter **MUSS** ein TLS-Zertifikat CLS_HAN_TLS_CRT$_{n+1}$ mit CLS_HAN_TLS_PUB/PRV$_{n+1}$ mit Zertifikatsprofil gemäß [DS] Kapitel HAN-Zertifikatsprofile CT_Selfsigned (Typ A) Funktion "cls", erzeugen, persistieren und im nächsten TLS-Handshake verwenden. [REQ.FA.CreateClsKeyPairAndCert.30]

Der CLS-Kommunikationsadapter **MUSS** das erzeugte CLS_HAN_TLS_CRT$_{n+1}$ an den Aufrufer des FA übermitteln. [REQ.FA.CreateClsKeyPairAndCert.40]

3.2.3.4 Implementierungshinweise

Der CLS-Kommunikationsadapter verwendet das CLS_HAN_TLS_CRT$_{n+1}$ künftig zur Authentisierung im TLS-Handshake, sofern nicht das SMGW im TLS-Handshake gemäß Detailspezifikation [DS] Kapitel TLS über die unterstützen CA *SubjectDN* signalisiert, das bisherige CLS_HAN_TLS_CRT$_n$ für die Authentisierung zu verwenden.

Dieser FA löscht nicht das bisherige CLS_HAN_TLS_CRT$_n$. Es kann gelöscht werden, wenn das neue CLS_HAN_TLS_CRT$_{n+1}$ zu einem erfolgreichen Verbindungsaufbau geführt hat und nicht mehr zur Kommunikation mit weiteren HAN-Teilnehmern benötigt wird.

Initiales Schlüsselpaar und Zertifikat CLS_HAN_TLS_PRV/PUB/CRT$_0$ sollen nicht gelöscht werden, da sie für ein erneutes Pairing benötigt werden. Die zeitliche Gültigkeit des Zertifikates wird nicht geprüft, da dieses ausschließlich zum initialen Pairing mit dem SMGW vorgesehen ist.

3.2.4 FA.ImportClsKeyPairAndCert

3.2.4.1 Beschreibung

Dieser FA beschreibt den Import eines durch das SMGW erzeugten Schlüsselpaares CLS_HAN_TLS_PRV/PUB$_{n+1}$ und des zugehörigen Zertifikates CLS_HAN_TLS_CRT$_{n+1}$ in den CLS-Kommunikationsadapter (in ▸Abschnitt 3.2.1.2 mit **ClsKeyGen SMGW** bezeichnet).

Damit kann der CLS-Kommunikationsadapter die vertrauenswürdigen Dienste zur Erzeugung der kryptografischen Schlüssel und des selbstsignierten CLS_HAN_TLS_CRT für eine automatisierte Aktualisierung verwenden, sofern das SMGW den Dienst anbietet.

Es gelten folgende Annahmen:

- Der Import geschieht über eine beidseitig authentifizierte, vertrauliche TLS-Verbindung gemäß [TR-03109-1] HAN-Kommunikationsszenario.
- Die kryptografischen Verfahren gemäß [TR-03109-3] werden verwendet.
- Das Zertifikat entspricht dem HAN-Zertifikatsprofil CT_Selfsigned (Typ A), Funktion "cls"
- Der Zufallszahlengenerator für die Schlüsselerzeugung entspricht den Vorgaben von [TR-03116-4] Kapitel 7

Dieses initiale CLS_HAN_TLS_CRT$_0$ Zertifikat wird zum initialen Aufbau einer vertraulichen TLS-Verbindung und zur Authentifizierung des CLS-Kommunikationsadapters durch das SMGW verwendet.

Da die kryptographischen Verfahren zur Validierung des Zertifikates gemäß [TR-03109-3] eine begrenzte Verwendbarkeit haben, muss ein Wechselprozess existieren, mit dem das Schlüsselpaar CLS_HAN_TLS_PRV/PUB und das zugehörige Zertifikat CLS_HAN_TLS_CRT erneuert und dem SMGW mitgeteilt werden.

3.2.4.2 Auslöser

REQ.FA.ImportClsKeyPairAndCert.10

Der CLS-Kommunikationsadapter **MUSS** den FA bei den in ▸ICS.FA.ImportClsKeyPairAndCert.10 beschriebenen Ereignissen auslösen.

ICS.FA.ImportClsKeyPairAndCert.20

Der Hersteller **MUSS** im ICS deklarieren, durch welche Ereignisse und Akteure der Import eines neuen CLS_HAN_TLS_CRT$_{n+1}$ und des zugehörigen Schlüsselpaares ausgelöst werden kann (mindestens eines). Ein solches Ereignis kann dabei auch durch den CLS-Kommunikationsadapter selbst ausgelöst werden. Wird ein Ereignis durch einen Akteur ausgelöst, der nicht der CLS-Kommunikationsadapter selbst ist, so **MUSS** der Hersteller im ICS deklarieren, wie Akteur und CLS-Kommunikationsadapter miteinander kommunizieren und über welche Schnittstelle bzw. welches Kommunikationsszenario diese Kommunikation geschieht.

3.2.4.3 Anforderungen

REQ.FA.ImportClsKeyPairAndCert.30

Der CLS-Kommunikationsadapter **MUSS** den Import ablehnen, sofern der Aufrufparameter nicht gültig ist:

- CLS_HAN_TLS_PRV oder CLS_HAN_TLS_CRT (mit CLS_HAN_TLS_PUB) fehlt im Aufrufparameter,
- die Signatur des Zertifikates kann nicht mit CLS_HAN_TLS_PUB validiert werden,
- Das Zertifikat entspricht nicht den Anforderungen eines HAN-Zertifikatsprofils gemäß [DS] Kapitel HAN-Zertifikatsprofile CT_Selfsigned (Typ A) Funktion "cls".
- Zur Überprüfung der Korrektheit des Schlüsselpaares: Eine mit dem privaten Schlüssel CLS_HAN_TLS_PRV signierte Nachricht kann nicht mit dem CLS_HAN_TLS_PUB des CLS_HAN_TLS_CRT validiert werden.

Der CLS-Kommunikationsadapter **MUSS** die Erzeugung von Schlüsselpaar und Zertifikat über ▸Kommunikationsszenario HKS.WS1.CLI: Nutzung von Webservices des SMGW mit Authentifizierung durch TLS-Client-Zertifikat für den SMGW-Dienst FA.DoCreateKeyPairAndCert auslösen. [REQ.FA.ImportClsKeyPairAndCert.40]

Der CLS-Kommunikationsadapter **MUSS** das über ▸Abschnitt 4.4.9 erhaltene Schlüsselpaar und Zertifikat gemäß ▸Abschnitt 3.2.8.1 persistieren und in allen folgenden TLS-Handshakes gemäß ▸Abschnitt 4.4 verwenden. [REQ.FA.ImportClsKeyPairAndCert.50]

Der CLS-Kommunikationsadapter **MUSS** das erzeugte CLS_HAN_TLS_CRT$_{n+1}$ an den Aufrufer des FA übermitteln. [REQ.FA.ImpotClsKeyPairAndCert.60]

3.2.4.4 Implementierungshinweise

Der CLS-Kommunikationsadapter verwendet das CLS_HAN_TLS_CRT$_{n+1}$ künftig zur Authentisierung im TLS-Handshake, sofern nicht das SMGW im TLS-Handshake gemäß Detailspezifikation [DS] Kapitel TLS über "Certificate_Authorities" signalisiert, das bisherige CLS_HAN_TLS_CRT$_n$ für die Authentisierung zu verwenden.

Dieser FA löscht nicht das bisherige CLS_HAN_TLS_CRT$_n$. Das Zertifikat kann gelöscht werden, wenn das neue CLS_HAN_TLS_CRT$_{n+1}$ zu einem erfolgreichen Verbindungsaufbau geführt hat und nicht mehr zur Kommunikation mit weiteren HAN-Teilnehmern benötigt wird.

Das CLS_HAN_TLS_CRT$_0$ wird nicht gelöscht, da es für ein erneutes Pairing - z.B. mit einem anderen SMGW - benötigt werden kann.

3.2.5 FA.PinSmgwCertificate

3.2.5.1 Beschreibung

Die TLS-Transportsicherung der Kommunikation mit dem SMGW basiert auf einer beidseitig zertifikatsbasierten Authentifizierung. Wird dieser FA durch einen berechtigten Akteur in einer definierten und zeitlich begrenzten Phase aufgerufen, persistiert der CLS-Kommunikationsadapter ein vom SMGW präsentiertes GW_HAN_TLS_CRT$_n$ als Vertrauensanker, der in nachfolgenden TLS-Handshakes zur Validierung und Authentifizierung des SMGW dient (Direct-Trust). Auch ein GW_HAN_TLS_CRT C_{TLS}(SMGW) der SM-PKI kann gepinnt werden.

Dieser FA kann bei der Erstinbetriebnahme aufgerufen werden, sofern kein *Vertrauensanker* des GW_HAN_TLS_CRT im CLS-Kommunikationsadapter bekannt ist (Auslieferungszustand, siehe auch ▸Abschnitt 3.3.1).

3.2.5.2 Auslöser

REQ.FA.PinSmgwCertificate.10

Der CLS-Kommunikationsadapter **MUSS** den FA bei den in ▸ICS.FA.PinSmgwCertificate.10 beschriebenen Ereignissen auslösen.

Beispiele für eine Auslösung können der Empfang einer Nachricht zum "Pinning" über den TLS-Proxy-Kanal, oder der Start des CLS-Kommunikationsadapters ohne bekannten SMGW-Vertrauensanker sein.

ICS.FA.PinSmgwCertificate.10

Der Hersteller **MUSS** im ICS deklarieren, durch welche Ereignisse und berechtigten Akteure das Zertifikats-Pinning für GW_HAN_TLS_CRT ausgelöst werden kann (mindestens eines). Ein solches Ereignis kann dabei auch durch den CLS-Kommunikationsadapter selbst ausgelöst werden. Wird ein Ereignis durch einen Akteur ausgelöst, der nicht der CLS-Kommunikationsadapter selbst ist, so **MUSS** der Hersteller im ICS deklarieren, wie Akteur und CLS-Kommunikationsadapter miteinander kommunizieren und über welche Schnittstelle bzw. welches Kommunikationsszenario diese Kommunikation geschieht. Die Berechtigungsprüfung ist im ICS zu beschreiben.

ICS.FA.PinSmgwCertificate.20

Der Hersteller **MUSS** im ICS deklarieren, ob das Pinning eines neuen SMGW-TLS-Zertifikates auch erfolgt, wenn bereits ein SMGW-TLS-Zertifikat persistiert ist.

3.2.5.3 Anforderungen

Der CLS-Kommunikationsadapter **MUSS** direkt nach Auslösen des FA für die in ▸ICS.FA.PinSmgwCertificate.30 festgelegte Dauer in einen Zustand gehen (Siehe ▸ICS.FA.PinSmgwCertificate.10), in dem das beim nächstem TLS-Handshake mit dem SMGW präsentierte TLS-Zertifikat, das sich von GW_HAN_TLS_CERT$_n$ unterscheidet, als SMGW-Vertrauensanker GW_HAN_TLS_CRT$_{n+1}$ verwendet ("gepinnt") wird. [REQ.FA.PinSmgwCertificate.20]

Der CLS-Kommunikationsadapter **MUSS** in dem in ▸REQ.FA.PinSmgwCertificate.20 genannten Zustand das im nächsten HAN-TLS-Handshake empfangene bisher nicht bekannte TLS-Client- oder Server-Zertifikat, als GW_HAN_TLS_CRT$_{n+1}$ persistieren und nach Ende eines Überlappungszeitraumes ausschließlich für die TLS-Authentifizierung des SMGW in folgenden TLS-Handshakes (Siehe ▸Abschnitt 4.4) verwenden. [REQ.FA.PinSmgwCertificate.30]

Sofern der CLS-Kommunikationsadapter bereits einem SMGW-Vertrauensanker ($GW\_HAN\_TLS\_CRT_n$ oder SM-PKI-CA-Zertifikat) vertraut, **MUSS** der CLS-Kommunikationsadapter in einem Überlappungszeitraum gemäß ▸ICS.FA.PinSmgwCertificate.40 im TLS-Handshake sowohl das bisherige als auch durch diesen FA gepinnte $GW\_HAN\_TLS\_CRT_{n+1}$ zur Validierung verwenden können. [REQ.FA.PinSmgwCertificate.40]

ICS.FA.PinSmgwCertificate.30

Der Hersteller **MUSS** im ICS deklarieren, wie viele Stunden nach Auslösen des FA der CLS-Kommunikationsadapter im Zustand verbleibt, in dem er offen für ein Zertifikats-Pinning des im TLS-Handshake vom SMGW präsentierten $GW\_HAN\_TLS\_CRT_{n+1}$ ist.

ICS.FA.PinSmgwCertificate.40

Der Hersteller **MUSS** im ICS deklarieren, wie lang (in Stunden) der CLS-Kommunikationsadapter im Zustand verbleibt, gemäß ▸REQ.FA.PinSmgwCertificate.40 im HAN-TLS-Handshake mehrere SMGW-Vertrauensanker validieren zu können.

3.2.5.4 Implementierungshinweise

Der CLS-Kommunikationsadapter signalisiert ab dem nächsten TLS-Handshake gemäß Detailspezifikation [DS] Kapitel TLS den *SubjectDN* der im CLS-Kommunikationsadapter gespeicherten *Vertrauensanker* (CA-Zertifikate).

3.2.6 FA.ImportSmgwTrustAnchor

3.2.6.1 Beschreibung

Die TLS-Transportsicherung der Kommunikation mit dem SMGW basiert auf einer beidseitig zertifikatsbasierten Authentifizierung. Dieser FA beschreibt die Anforderungen an den Import eines Zertifikates, mit dem das vom SMGW im TLS-Handshake präsentierte GW_HAN_TLS_CRT validiert werden kann, um die Authentizität des SMGW zu gewährleisten.

Ein berechtigter Akteur kann dazu entweder ein individuelles GW_HAN_TLS_CRT gemäß Detailspezifikation [DS] Kapitel HAN-Zertifikatsprofile CT_Selfsigned (Typ A) oder CT_SMPKI_Signed (Typ C) oder ein Root- oder Sub-CA-Signatur-Zertifikat der SM-PKI gemäß [TR-03109-4] importieren und aktivieren.

Dieser FA kann beispielsweise in folgenden Situationen aufgerufen werden:

- Vorbereitend zur ersten Kommunikation mit dem SMGW (Erstkonfiguration)
- Vorbereitend zu oder nach einem Wechsel des CA-Zertifikates
- Vorbereitend zu einem Wechsel des SMGW

3.2.6.2 Auslöser

REQ.FA.ImportSmgwTrustAnchor.5

Der CLS-Kommunikationsadapter **MUSS** den FA bei den in ▸ICS.FA.ImportSmgwTrustAnchor.10 beschriebenen Ereignissen auslösen.

ICS.FA.ImportSmgwTrustAnchor.10

Der Hersteller **MUSS** im ICS deklarieren, durch welche Ereignisse und berechtigten Akteure der Import des Vertrauensankers zur Validierung des vom SMGW präsentierten GW_HAN_TLS_CRT ausgelöst werden kann (mindestens ein Ereignis sowie berechtigter Akteur). Wird ein Ereignis durch einen Akteur ausgelöst, der nicht der CLS-Kommunikationsadapter selbst ist, so **MUSS** der Hersteller im ICS deklarieren, wie Akteur und CLS-Kommunikationsadapter miteinander kommunizieren und über welche Schnittstelle bzw. welches Kommunikationsszenario diese Kommunikation geschieht. Die Berechtigungsprüfung ist im ICS zu beschreiben.

3.2.6.3 Anforderungen

Der CLS-Kommunikationsadapter **MUSS** den über die Schnittstelle gemäß ▸ICS.FA.ImportSmgwTrustAnchor.10 empfangenen Vertrauensanker zur Validierung des GW_HAN_TLS_CRT ablehnen, sofern dessen Syntax nicht den Vorgaben gemäß Detailspezifikation [DS] Kapitel HAN-Zertifikatsprofile Typ A (Direct-Trust) oder einem Root- oder Sub-CA-Zertifikat der SM-PKI gemäß [TR-03109-4] entspricht. [REQ.FA.ImportSmgwTrustAnchor.10]

Der CLS-Kommunikationsadapter **MUSS** zwei Vertrauensanker zur Validierung des *GW_HAN_TLS_CRT* gleichzeitig unterstützen, um während eines Wechselprozesses einen Überlappungszeitraum zu ermöglichen, in dem CLS-Kommunikationsadapter und SMGW zeitgleich den bisherigen und künftigen Vertrauensanker besitzen. [REQ.FA.ImportSmgwTrustAnchor.20]

Der CLS-Kommunikationsadapter **MUSS** den validen Vertrauensanker persistieren und für die künftige Validierung des GW_HAN_TLS_CRT verwenden. [REQ.FA.ImportSmgwTrustAnchor.30]

Sofern der CLS-Kommunikationsadapter bereits einem SMGW-Vertrauensanker ($GW\_HAN\_TLS\_CRT_n$ oder SM-PKI-CA-Zertifikat) vertraut, **MUSS** der CLS-Kommunikationsadapter in einem Überlappungszeitraum gemäß ▸ICS.FA.ImportSmgwTrustAnchor.10 im TLS-Handshake sowohl das bisherige als auch das durch diesen FA importierte GW_HAN_TLS_CRT oder CA-Zertifikat zur Validierung verwenden können. [REQ.FA.ImportSmgwTrustAnchor.40]

ICS.FA.ImportSmgwTrustAnchor.20

Der Hersteller **MUSS** im ICS deklarieren, wie lang (in Stunden) der CLS-Kommunikationsadapter im Zustand verbleibt, gemäß ▸REQ.FA.ImportSmgwTrustAnchor.40 im HAN-TLS-Handshake mehrere SMGW-Vertrauensanker validieren zu können.

3.2.7 FA.DeactivateSmgwTrustAnchor

3.2.7.1 Beschreibung

Nach Aufruf dieses FA kann ein im CLS-Kommunikationsadapter persistierter (nicht mehr gültiger) *Vertrauensanker* nicht mehr zur Überprüfung der Authentizität von (SMGW-TLS-)Zertifikaten verwendet werden.

Durch den FA können vom Hersteller installierte Vertrauensanker und die durch ▸FA.PinSmgwCertificate oder durch ▸FA.ImportSmgwTrustAnchor persistierten, gelöscht werden.

Dieser FA kann in unterschiedlichen Phasen des Lebenszyklus aufgerufen werden:

- Zum Deaktivieren des bisherigen Zertifikates nach erfolgreichem Wechsel eines GW_HAN_TLS_CRT bzw. dessen CA-Zertifikates eines SMGW bei einem nicht automatisierten Wechselprozess.
- Zum Deaktivieren eines Vertrauensankers, sofern der CLS-Kommunikationsadapter mehrere Vertrauensanker besitzt.
- Zum Deaktivieren des Zertifikates eines bisherigen SMGW, sofern der CLS-Kommunikationsadapter im Rahmen eines Wechselprozesses mit einem anderen SMGW assoziiert wird.

3.2.7.2 Auslöser

REQ.FA.DeactivateSmgwTrustAnchor.10

Der CLS-Kommunikationsadapter **MUSS** den FA bei den in ▸ICS.FA.DeactivateSmgwTrustAnchor.10 beschriebenen Ereignissen auslösen.

ICS.FA.DeactivateSmgwTrustAnchor.10

Der Hersteller **MUSS** im ICS beschreiben, durch welche Ereignisse und berechtigten Akteure der Vertrauensanker zur Validierung des vom SMGW präsentierten GW_HAN_TLS_CRT deaktiviert werden kann (mindestens eines). Ein solches Ereignis kann dabei auch durch den CLS-Kommunikationsadapter selbst ausgelöst werden. Wird ein Ereignis durch einen Akteur ausgelöst, der nicht der CLS-Kommunikationsadapter selbst ist, so **MUSS** der Hersteller im ICS deklarieren, wie Ak-

teur und CLS-Kommunikationsadapter miteinander kommunizieren und über welche Schnittstelle bzw. welches Kommunikationsszenario diese Kommunikation geschieht. Die Berechtigungsprüfung ist im ICS zu beschreiben.

3.2.7.3 Anforderungen

Der CLS-Kommunikationsadapter **DARF** den deaktivierten Vertrauensanker zur Überprüfung der Authentizität des SMGW **NICHT** mehr für die künftige Validierung von im TLS-Handshake präsentierten TLS-Client- oder TLS-Server-Zertifikaten oder zur Berechtigungsprüfung verwenden. [REQ.FA.DeactivateSmgwTrustAnchor.20]

ICS.FA.DeactivateSmgwTrustAnchor.20

Der Hersteller **MUSS** im ICS beschreiben, welche Vertrauensanker zur Validierung von SMGW-TLS-Zertifikaten als Default vorinstalliert sind.

3.2.7.4 Implementierungshinweise

Zur Verbesserung der Wechselprozesssicherheit sollte ein Aufrufparameter dieses FA das zu deaktivierende GW_HAN_TLS_CRT identifizieren, so dass nur das identifizierte Zertifikat deaktiviert wird.

3.2.8 Datenstrukturen

3.2.8.1 Zertifikat und Schlüssel

Diese Datenstruktur enthält einen privaten Schlüssel und das zugehörige Zertifikat als Ergebnis des Zertifikatserstellungsdienstes des SMGW.

Das SMGW **MUSS** das Ergebnis der Zertifikatserstellung für CLS gemäß ▸Tabelle 3.2 bereitstellen. [REQ.FAKAT.ClsServices.40]

Datenfeld	Datentyp	Beschreibung
Zertifikat (cert)	String (hexstring)	Dieses Datenfeld enthält das gemäß [RFC5280] in ASN.1, [X.690] DER codierte X.509 Zertifikat zum privaten Schlüssel des Datenfeldes "privateKey".
Privater Schlüssel (privateKey)	String (hexstring)	Dieses Datenfeld enthält den gemäß [RFC5915] in ASN.1, [X.690] DER codierte privaten Schlüssel des Datenfeldes "cert".

Tabelle 3.2 Datenfelder Zertifikat und Schlüssel

3.3 FA-Kategorie Konfiguration

Diese FA-Kategorie beschreibt die mindestens erforderlichen Fachanwendungsfälle zur Konfiguration eines CLS-Kommunikationsadapters.

Aufgabe	Umsetzung
Zurücksetzen der Konfiguration auf Voreinstellungen	Der CLS-Kommunikationsadapter **MUSS** ▸FA.RestoreDefaults implementieren. [REQ.FAKAT.Config.10]

Tabelle 3.3 Übersicht über die FA zur Konfiguration eines CLS-Kommunikationsadapters

3.3.1 FA.RestoreDefaults

3.3.1.1 Beschreibung

Dieser FA beschreibt die funktionalen Anforderungen an die Herstellung eines Zustandes des CLS-Kommunikationsadapters, der dem Auslieferungszustand am Einbauort entspricht. Dabei werden eventuell vorhandene kommunikative Anbindungen an das SMGW aufgehoben. Die Firmwareversion wird dabei nicht verändert.

Anschließend kann der CLS-Kommunikationsadapter über eine initiale kommunikative Anbindung (erneut) mit einem SMGW assoziiert werden.

Der FA wird durch einen *Kommunikationspartner im WAN* sowie optional über ein lokales Ereignis ausgelöst, falls die Kommunikation über das SMGW nicht möglich ist.

3.3.1.2 Auslöser

REQ.FA.RestoreDefaults.10

Der CLS-Kommunikationsadapter **SOLL** den FA bei folgenden Ereignissen auslösen:

- Empfang einer Nachricht gemäß ▸ICS.FA.RestoreDefaults.10
- Physisches, lokales Ereignis gemäß ▸ICS.FA.RestoreDefaults.20

ICS.FA.RestoreDefaults.10

Der Hersteller **MUSS** im ICS deklarieren, durch welches informationstechnische Ereignis (Nachricht, berechtigter Akteur) dieser FA durch den *Kommunikationspartner im WAN* ausgelöst werden kann (Mindestens eins).

ICS.FA.RestoreDefaults.20

Der Hersteller **MUSS** im ICS deklarieren, ob der FA durch ein lokales Ereignis ausgelöst werden kann. Sofern dies möglich ist, **MUSS** der Hersteller im ICS deklarieren, durch welches Ereignis, welchen Akteur und wie dieses Ereignis ausgelöst wird.

ICS.FA.RestoreDefaults.30

Der Hersteller **MUSS** im ICS deklarieren, welche Datenobjekte durch diesen FA auf Default-Werte zurückgesetzt (bzw. gelöscht) werden und die Default-Werte beschreiben. Mindestens sind die Default-Werte für den Prüfgegenstand und für folgende Datenobjekte zu beschreiben:

- HAN-Interface-Konfiguration (Layer 1-2 Parameter, Netzwerk-Layer (z.B. Bezug von IP-Adressen), Ports)
- Vertrauensanker
- CLS-Zertifikate
- personenbeziehbare Daten, die nach der Installation erfasst wurden.

3.3.1.3 Anforderungen

Der CLS-Kommunikationsadapter **MUSS** in einen Zustand gehen, in dem die erneute kommunikative Anbindung über ▸FA.PinSmgwCertificate an ein SMGW möglich ist. [REQ.FA.RestoreDefaults.20]

Der CLS-Kommunikationsadapter **MUSS** die in ▸ICS.FA.RestoreDefaults.30 genannten Datenobjekte auf die in dem ICS genannten Default-Werte zurücksetzen. [REQ.FA.RestoreDefaults.30]

3.3.1.4 Implementierungshinweise

Der Hersteller sollte in den Handbüchern erläutern, welche Daten und Konfigurationen durch diesen FA gelöscht werden. Wenn dieser FA genutzt werden soll, um den Zugriff auf Daten irreversibel zu verhindern, so kann dies durch Löschen der Daten oder der Schlüssel zum Zugriff auf diese Daten verhindert werden.

Nicht mehr benötigte Schlüssel und Zertifikate sollten gelöscht werden.

Damit im Anschluss eine (erneute) Anbindung an ein SMGW möglich ist, sollte der private Schlüssel $CLS\_HAN\_TLS\_PRV_0$ zum Initialen Pairing-Zertifikat $CLS\_HAN\_TLS\_CRT_0$ nicht gelöscht werden.

3.4 FA-Kategorie Nutzung eines sicheren transparenten Kanals

3.4.1 Einleitung

Der TLS-Proxy-Kanal ist ein vom SMGW vermittelter, TLS-gesicherter Kommunikationskanal zwischen einem CLS-Kommunikationsadapter und einem Kommunikationspartner im WAN[7] des SMGW, der durch die TLS-Proxy-Funktion des SMGW realisiert ist. Dazu wird eine *TLS-Verbindung* zwischen SMGW und CLS-Kommunikationsadapter (sowie zwischen SMGW und Kommunikationspartner im WAN) aufgebaut.

Die FA-Kategorie beschreibt, wie ein CLS-Kommunikationsadapter die TLS-Verbindung zum Aufbau eines TLS-Proxy-Kanals initiiert bzw. eine Aufforderung dazu empfängt und umsetzt sowie die Nutzung des TLS-Proxy-Kanals.

Aufgabe	Umsetzung
Aufbau einer TLS-Proxy-Verbindung zum SMGW, initiiert durch den CLS-Kommunikationsadapter	Der CLS-Kommunikationsadapter **SOLL** ▸FA.RequestProxyCh initiiert durch den CLS-Kommunikationsadapter implementieren. (Siehe ▸ICS.IOP.HKS.TLSPROXY.20) [REQ.FAKAT.TlsProxy.10]
Aufbau einer TLS-Proxy-Verbindung zum CLS-Kommunikationsadapter, initiiert durch das SMGW	Der CLS-Kommunikationsadapter **SOLL** ▸FA.AcceptProxyCh implementieren. (Siehe ▸ICS.IOP.HKS.TLSPROXY.10) [REQ.FAKAT.TlsProxy.20]
Beenden einer TLS-Proxy-Verbindung durch den CLS-Kommunikationsadapter	Der CLS-Kommunikationsadapter **MUSS** ▸FA.CloseProxyCh, initiiert durch den CLS-Kommunikationsadapter implementieren. [REQ.FAKAT.TlsProxy.30]
Beenden einer TLS-Proxy-Verbindung durch das SMGW	Der CLS-Kommunikationsadapter **MUSS** ▸FA.CloseProxyCh, initiiert durch das SMGW implementieren. [REQ.FAKAT.TlsProxy.40]

Tabelle 3.4 Übersicht über die FA zur Nutzung eines sicheren transparenten Kanals

Der CLS-Kommunikationsadapter **MUSS** entweder ▸FA.RequestProxyCh oder ▸FA.AcceptProxyCh implementieren. [REQ.FAKAT.TlsProxy.50]

3.4.2 FA.RequestProxyCh

3.4.2.1 Beschreibung

Dieser FA beschreibt die Anforderungen an das Aufbauen eines TLS-Proxy-Kanals zwischen einem CLS-Kommunikationsadapter und einem Kommunikationspartner im WAN, initiiert durch den CLS-Kommunikationsadapter, damit der Kommunikationspartner im WAN und der CLS-Kommunikationsadapter Informationen austauschen können. Der CLS-Kommunikationsadapter signalisiert dem SMGW über eine über Standards vereinbarte oder bei der Bestellung vorkonfigurierte *ProxyId*, welches Proxy-Kommunikationsprofil zum Aufbau einer TLS-Verbindung zum Kommunikationspartner im WAN ausgewählt wird.

3.4.2.2 Auslöser

REQ.FA.RequestProxyCh.10

Der CLS-Kommunikationsadapter **MUSS** den FA bei einem in ▸ICS.FA.RequestProxyCh.10 beschriebenen Ereignis auslösen.

ICS.FA.RequestProxyCh.10

Der Hersteller **MUSS** im ICS deklarieren, durch welches (testbare) Ereignis der ▸FA.RequestProxyCh ausgelöst wird, so dass ein TLS-Proxy-Kanal zum SMGW initiiert wird.

[7] Gemäß [TR-03109-1] also ein *aEMT*.

3.4.2.3 Anforderungen

Der CLS-Kommunikationsadapter **MUSS** die TLS-Verbindung zum SMGW über ▸HKS.TLSPROXY.SOCKSCLI oder ▸HKS.TLSPROXY.CLI aufbauen. [REQ.FA.ProxyRequestCh.20]

Der CLS-Kommunikationsadapter **MUSS** mindestens zwei TLS-Proxy-Verbindungen zum SMGW gleichzeitig unterstützen. [REQ.FA.ProxyRequestCh.30]

ICS

ICS.FA.RequestProxyCh.20

Der Hersteller **MUSS** im ICS deklarieren, wie viele gleichzeitige TLS-Proxy-Verbindungen zum SMGW der CLS-Kommunikationsadapter unterstützt.

3.4.3 FA.AcceptProxyCh

3.4.3.1 Beschreibung

Dieser FA beschreibt die Anforderungen an das Aufbauen eines TLS-Proxy-Kanals zwischen CLS-Kommunikationsadapter und einem Kommunikationspartner im WAN, initiiert durch das SMGW, damit der Kommunikationspartner im WAN und der CLS-Kommunikationsadapter Informationen austauschen können.

3.4.3.2 Auslöser

REQ.FA.AcceptProxyCh.10

Der CLS-Kommunikationsadapter **MUSS** den FA bei folgendem Ereignis auslösen:

- Empfang einer Verbindungsanforderung über ▸HKS.TLSPROXY.SRV

3.4.3.3 Anforderungen

Der CLS-Kommunikationsadapter **MUSS** den Verbindungsaufbau gemäß ▸Abschnitt 4.4.6: HKS.TLSPROXY.SRV durchführen. [REQ.FA.AcceptProxyCh.20]

3.4.4 FA.CloseProxyCh

3.4.4.1 Beschreibung

Die TLS-Verbindung zum SMGW, die einem TLS-Proxy-Kanal zugeordnet ist, wird beendet.

3.4.4.2 Auslöser

REQ.FA.CloseProxyCh.10

Der CLS-Kommunikationsadapter **MUSS** den FA bei folgenden Ereignissen auslösen:

- Empfang einer CloseNotify-Anforderung in einer ▸HKS.TLSPROXY.CLI Verbindung
- Empfang einer CloseNotify-Anforderung in einer ▸HKS.TLSPROXY.SRV Verbindung
- Empfang einer CloseNotify-Anforderung in einer ▸HKS.TLSPROXY.SOCKSCLI Verbindung
- Ereignis im CLS-Kommunikationsadapter gemäß ▸ICS.FA.CloseProxyCh.10

ICS.FA.CloseProxyCh.10

Der Hersteller **MUSS** im ICS deklarieren, durch welches (testbare) Ereignis der ▸FA.CloseProxyCh ausgelöst wird, der einen TLS-Proxy-Kanal zum SMGW beendet. Dieses ICS bleibt leer, wenn kein Ereignis des CLS-Kommunikationsadapters zum Beenden des TLS-Proxy-Kanals führt.

3.4.4.3 Anforderungen

Der CLS-Kommunikationsadapter **MUSS** die TLS-Verbindung zum SMGW beenden, die dem auslösenden Ereignis zugeordnet ist. [REQ.FA.CloseProxyCh.20]

3.5 FA-Kategorie Zeitführung

3.5.1 Beschreibung

Ein CLS-Kommunikationsadapter kann für fachliche Zwecke, z.B. für Zeitstempelungen bei Protokollierung, zeitliche Gültigkeitsprüfungen, zeitsynchrone Steuerungen einen Bezug zur aktuellen Zeit benötigen.

Die FA-Kategorie beschreibt, wie der CLS-Kommunikationsadapter von einem Zeitserver authentisch und zuverlässig die Systemzeit erhält.

▸Abbildung 3.7 ordnet den CLS-Kommunikationsadapter in die Zeitsynchronisations-Hierarchie des Intelligenten Messsystems ein. Die Referenzzeit (Stratum 0) ist die nationale gesetzliche Zeit.

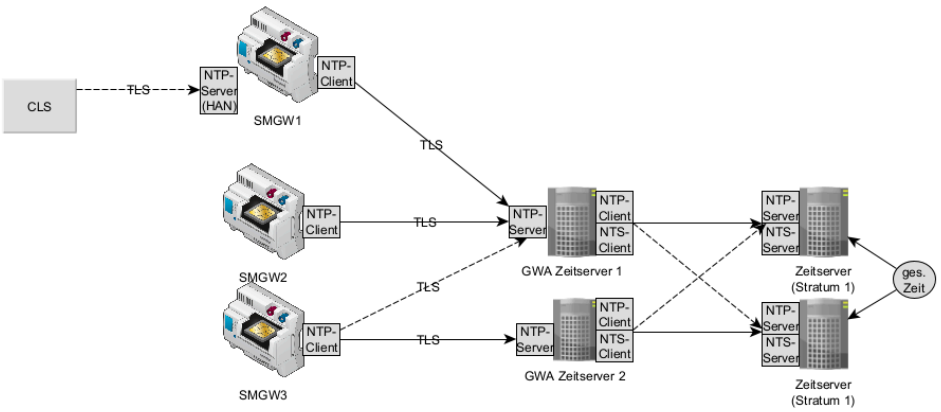

Abbildung 3.7. Synchronisationshierarchie des Intelligenten Messsystems

Aufgabe	Umsetzung
Bezug der Systemzeit und Führung der Systemzeit durch den CLS-Kommunikationsadapter	Der CLS-Kommunikationsadapter **MUSS** ▸FA.DoTimeSync implementieren. [REQ.FAKAT.TimeSync.10]

Tabelle 3.5 Übersicht über die FA zur Zeitführung

3.5.2 FA.DoTimeSync

3.5.2.1 Beschreibung

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

Die Round-Trip-Time (RTT) bzw. die gesamte Verzögerung zwischen CLS-Kommunikationsadapter und Zeitserver ist in der Regel für die Genauigkeit der Synchronisation unerheblich, solange gewährleistet ist, dass die Verzögerungen auf dem Hin- und Rückweg vom Zeitserver ungefähr gleich sind. Zur Vermeidung von Fehl-Synchronisationen verwirft der CLS-Kommunikationsadapter Antworten, die zu stark verzögert sind.

Der CLS-Kommunikationsadapter bestimmt die Zeitabweichung zwischen Systemzeit und Referenzzeit aus den vom NTP-Protokoll bereitgestellten Informationen.

3.5.2.2 Auslöser

REQ.FA.DoTimeSync.10

Der CLS-Kommunikationsadapter **MUSS** den Verbindungsaufbau zur Zeitsynchronisation bei folgenden Ereignissen auslösen:

- randomisiert innerhalb von 30 Minuten nach Neustart der Komponente und Erreichen der Betriebsbereitschaft
- periodisch gemäß ▸ICS.FA.DoTimeSync.10

3.5.2.3 Anforderungen

Der CLS-Kommunikationsadapter **MUSS** die Systemzeit regelmäßig synchronisieren. (Siehe ▸ICS.FA.DoTimeSync.10) [REQ.FA.DoTimeSync.20]

Der CLS-Kommunikationsadapter **MUSS** die regelmäßige Zeitsynchronisation gemäß ▸REQ.FA.DoTimeSync.20 über ▸HKS.NTP-TLS.CLI auslösen können. [REQ.FA.DoTimeSync.30]

Sofern die Zeitsynchronisation über ▸Abschnitt 4.4.8 nicht durchgeführt werden kann, **SOLL** der CLS-Kommunikationsadapter die Zeitsynchronisation über ▸HKS.TLSPROXY.CLI, ▸HKS.TLSPROXY.SOCKSCLI oder ▸HKS.TLSPROXY.SRV durchführen. [REQ.FA.DoTimeSync.35]

Sofern die Zeitsynchronisation mit dem SMGW oder über das SMGW nicht durchgeführt werden kann, **KANN** der CLS-Kommunikationsadapter die Zeitsynchronisation über weitere Schnittstellen durchführen. (▸ICS.FA.DoTimeSync.30) [REQ.FA.DoTimeSync.36]

Um Delay-Angriffe und Zeitmessungen mit zu langer RTT zu verwerfen, **MUSS** der CLS-Kommunikationsadapter NTP-Antworten verwerfen, die später als 9 Sekunden nach NTP-Anfrage eintreffen. [REQ.FA.DoTimeSync.40]

Der CLS-Kommunikationsadapter **MUSS** mindestens bis zum 31.12.2049 23:59:59 UTC die vom Zeitserver empfangene Zeit korrekt in die Systemzeit umwandeln können. [REQ.FA.DoTimeSync.50]

Der CLS-Kommunikationsadapter **MUSS** die empfangene Zeitinformation in die Systemzeit übernehmen. [REQ.FA.DoTimeSync.60]

ICS.FA.DoTimeSync.10

Der Hersteller **MUSS** im ICS deklarieren, wie häufig der CLS-Kommunikationsadapter im Regelfall die Systemzeit synchronisiert (in Stunden).

ICS.FA.DoTimeSync.20

Der Hersteller **MUSS** im ICS deklarieren, über welches HKS der CLS-Kommunikationsadapter die Zeitsynchronisation durchführen kann.

ICS.FA.DoTimeSync.30

Der Hersteller **MUSS** im ICS deklarieren, über welche weiteren Schnittstellen der CLS-Kommunikationsadapter die Systemzeit stellen oder synchronisieren kann.

3.5.2.4 Implementierungshinweise

Sofern bei der Kommunikation mit dem Zeitserver nicht vernachlässigbare Laufzeitunterschiede erwartet werden, sollte zur Verbesserung der Genauigkeit eine Zeitsynchronisation mit den Prozeduren gemäß [RFC5905] Kap. 9ff erfolgen. Bei Zeitsynchronisation im HAN des SMGW ist dies normalerweise nicht erforderlich, so dass eine SNTP-Funktionalität ausreichend ist.

Der CLS-Kommunikationsadapter soll im Regelfall zur zeitlichen Gültigkeitsprüfung von SM-PKI-Zertifikaten des SMGW einmal täglich die Zeit abfragen.

Die Zeitsynchronisationsanfrage des CLS-Kommunikationsadapters über HKS.NTP-TLS.CLI löst keinen WAN-Verbindungsaufbau im SMGW aus.

Gemäß [RFC5905] können die NTP-Variablen Root-Dispersion und Root-Delay zur Ermittlung des maximalen Fehlers zur Reference-Clock (Zeitserver Stratum 0) dienen.

3.6 FA-Kategorie Firmware-Update

3.6.1 Einleitung

Ein CLS-Kommunikationsadapter muss zur zeitnahen Behebung von Schwachstellen und Softwarefehlern sowie zur Änderung von Funktionalitäten - etwa, um den Funktionsumfang oder die Interoperabilität zu erhöhen - ein Firmware-Update ermöglichen.

Die FA-Kategorie beschreibt die dafür notwendigen Fachanwendungsfälle.

Über die Anforderungen in diesen FA hinaus sind die IT-Sicherheitsanforderungen bezüglich Firmware-Updates zu beachten, siehe ▸Kapitel 5.

Aufgabe	Umsetzung
Installation eines Firmware-Updates	Der CLS-Kommunikationsadapter **MUSS** ▸FA.FwInstallation implementieren. [REQ.FAKAT.FwUpdate.10]

Tabelle 3.6 Übersicht über die FA zum Firmware-Update

3.6.2 FA.FwInstallation

3.6.2.1 Beschreibung

Dieser FA beschreibt die funktionalen Anforderungen an die Funktionalität zur Installation eines *Firmware-Updates* für einen CLS-Kommunikationsadapter.

Der Installationsprozess kann nach dem Auslösen des FA verzögert werden, bis die Bedingungen für eine Installation erfüllt sind.

Es ist zu beachten, dass das Aktualisieren jeglicher *Firmware* auf der CLS-Komponente mittels der Firmware-Update-Funktionalität des CLS-Kommunikationsadapters durchgeführt werden muss.

3.6.2.2 Auslöser

REQ.FA.FwInstallation.10

Der CLS-Kommunikationsadapter **MUSS** den FA bei folgendem Ereignis auslösen:

- Empfang einer Nachricht gemäß ▸ICS.FA.FwInstallation.10

ICS.FA.FwInstallation.10

Der Hersteller **MUSS** im ICS deklarieren, durch welches informationstechnische Ereignis (Nachricht, Schnittstelle, berechtigter Akteur) die Installation eines Firmware-Updates ausgelöst werden kann (mindestens eines) und welche Bedingungen für die Installation erfüllt sein müssen.

3.6.2.3 Anforderungen

In Folge eines der in ▸ICS.FA.FwInstallation.10 deklarierten Ereignisse **MUSS** der CLS-Kommunikationsadapter mit dem Installationsprozess beginnen, wenn die im ICS genannten sonstigen Bedingungen erfüllt sind. Der CLS-Kommunikationsadapter **MUSS** dazu die folgenden Ablaufschritte umsetzen: [REQ.FA.FwInstallation.20]

1. Der CLS-Kommunikationsadapter prüft, ob der Akteur, der das Ereignis zur Installation ausgelöst hat, einem der in ▸ICS.FA.FwInstallation.10 deklarierten Akteure entspricht.

2. Der CLS-Kommunikationsadapter prüft das Firmware-Update mittels eines geeigneten Signaturverfahrens (siehe ▸ICS.FA.FwInstallation.50) auf Authentizität und Integrität.

   a. Der CLS-Kommunikationsadapter **MUSS** zur Prüfung der Authentizität und des Ursprungs der Firmware den öffentlichen Signatur-Schlüssel des Herstellers verwenden. [REQ.FA.FwInstallation.30]

3. Der CLS-Kommunikationsadapter prüft, ob die Version der Firmware im Firmware-Update neuer ist als die im CLS-Kommunikationsadapter vorhandene Version.

   a. Der Hersteller **MUSS** zur Unterstützung dieser Prüfung die Versionierung der Firmware gemäß *Semantic Versioning 2.0.0* verwenden. [REQ.FA.FwInstallation.40]

4. Schlägt eine der Prüfungen fehl, darf der CLS-Kommunikationsadapter das Firmware-Update nicht installieren.

5. Der CLS-Kommunikationsadapter aktualisiert bei erfolgreicher Prüfung von Authentizität, Integrität und Version des Firmware-Updates die Firmware auf Basis des Firmware-Updates und aktiviert die neue Firmware.

6. Der CLS-Kommunikationsadapter hält die vor dem Update bestehende Firmware als Ersatz für den Fehlerfall nach Installation des Firmware-Updates vor und verwendet diese, falls das Update fehlschlägt.

ICS.FA.FwInstallation.20

Der Hersteller **MUSS** im ICS beschreiben, wie eine Firmware-Datei in den CLS-Kommunikationsadapter übertragen wird.

ICS.FA.FwInstallation.30

Der Hersteller **MUSS** die kryptographischen Parameter für die Firmware-Signatur-Prüfung und die Struktur, den initialen Import, das Persistieren und die Aktualisierung des Vertrauensankers zur Signaturprüfung beschreiben.

ICS.FA.FwInstallation.40

Der Hersteller **MUSS** im ICS beschreiben, wie und über welche Schnittstelle der Komponente die aktive Firmware-Version des CLS-Kommunikationsadapters ermittelt werden kann.

ICS.FA.FwInstallation.50

Der Hersteller **MUSS** im ICS beschreiben, wie die Anforderungen der [TR-03116-4] Kapitel 7 an die Erzeugung, Speicherung und Löschung von privaten Firmware-Signaturschlüsseln umgesetzt sind.

4 Anforderungen an die Kommunikationsverbindungen und Protokolle

4.1 Einleitung

Dieser Abschnitt beschreibt die Interoperabilitäts-Anforderungen an die Protokolle von CLS-Kommunikationsadaptern, die für die Kommunikation mit dem SMGW benötigt werden.

Der CLS-Kommunikationsadapter verfügt über eine Schnittstelle zum SMGW, um mit dem SMGW (via IF_GW_CLS) in dessen HAN zu kommunizieren.

Die Technische Richtlinie verwendet das Konzept eines Kommunikationsszenarios zur strukturierten Beschreibung von Anforderungen an die Kommunikationsverbindungen des CLS-Kommunikationsadapters. Ein Kommunikationsszenario benennt für die Protokollschichten gemäß OSI 7-Schichten Modell einer logischen Schnittstelle die zu verwendenden Protokolle, Nachrichtenformate und die Rolle des CLS-Kommunikationsadapters gemäß Protokollschicht (z.B. Client/Server).

Die Kommunikationsszenarien referenzieren öffentlich zugängliche Schnittstellen-Protokoll-Spezifikationen, die idealerweise europäisch oder international im Konsens erarbeitet wurden. Anforderungen in den Kommunikationsszenarien konkretisieren, begrenzen oder erweitern die Universal-Anforderungen dieser Spezifikationen als Mindestanforderungen des BSI zur Interoperabilität des CLS-Kommunikationsadapters.

Detailspezifikationen ([DS]) konkretisieren die Anforderungen der referenzierten Schnittstellen-Protokoll-Spezifikationen (siehe ▸Abschnitt 4.3) zur Verbesserung der Interoperabilität im iMSys mit dem Ziel, die Austauschbarkeit und Wechselprozesse weiter zu verbessern. Diese Detailspezifikationen werden regelmäßig überprüft und im Bedarfsfall nach Erfahrungen von Herstellern und Anwendern aktualisiert.

4.2 Struktur der Kommunikationsszenarien

Die folgende Liste stellt die Informationen dar, die für jedes Kommunikationsszenario (KS) aufgeführt werden.

Beschreibung Die Beschreibung ist die ausführliche textuelle und grafische Darlegung der Aufgabe des KS. Sie dient vor allem dem Verständnis des KS und enthält die notwendigen Informationen, um Protokollstapel und Kommunikationsablauf des KS vollständig nachvollziehen zu können.

Vorbedingungen Dieser optionale Abschnitt enthält die wesentlichen Vorbedingungen, für den Informationsaustausch in diesem KS. Dieser Abschnitt entfällt, wenn keine wesentlichen Vorbedingungen zu berücksichtigen sind.

Sicherung der Kommunikation Dieser optionale Abschnitt beschreibt die für die Authentifizierung, Verschlüsselung und Autorisierung in den Sicherheitsprotokollen anzuwendenden Sicherheitsparameter, wie beispielsweise Anforderungen an die Zertifikatsprüfung oder die Nachrichtensicherung. Dieser Abschnitt entfällt, wenn das Kommunikationsszenario keinen Beitrag zur Sicherung der Kommunikation enthält.

Kommunikationsprotokolle Dieser Abschnitt referenziert die Spezifikationen der von diesem KS verpflichtend zu implementierenden Kommunikationsprotokolle und die Rolle des CLS-Kommunikationsadapters in der jeweiligen Protokollschicht.

Technische Anwendungsfälle Ein technischer Anwendungsfall (TA) beschreibt eine Protokollfunktionalität, wie Verbindungsaufbau oder Erstellen einer Nachricht für eine Kommunikationsdienstprimitive (Request, Response). Dieser Abschnitt listet die zu implementierenden technischen Anwendungsfälle, zu denen Detailspezifikationen zur Verbesserung der Interoperabilität weitere Anforderungen stellen können.

4.3 Mitgeltende Teile der Detailspezifikation zur TR-03109-5

▸Tabelle 4.1 enthält eine Übersicht der mitgeltenden Abschnitte der [DS], die Anforderungen zur Verbesserung der technischen Interoperabilität zwischen CLS-Kommunikationsadapter und SMGW enthalten.

ICS.IOP.KS.HAN.10

Der Hersteller **MUSS** im ICS deklarieren, zu welcher Version der Detailspezifikation er die Konformität der Protokolle und Datenstrukturen der Schnittstelle zum HAN des SMGW bestätigt.

Kapitel der DS	Relevante Teile	Kommunikationsszenario
HAN-Zertifikatsprofile	Verarbeitung von selbstsignierten SMGW-Zertifikaten CT_Selfsigned (Typ A) und SM-PKI-Zertifikaten des SMGW CT_SMPKI_Signed (Typ C), sowie Anforderungen an CLS-Zertifikate	▸HKS.NTP-TLS.CLI, ▸Kommunikationsszenario HKS.WS1.CLI: Nutzung von Webservices des SMGW mit Authentifizierung durch TLS-Client-Zertifikat, ▸HKS.TLSPROXY.SOCKSCLI, ▸HKS.TLSPROXY.SRV, ▸HKS.TLSPROXY.CLI
RESTful Webservice	Anforderungen an HTTP-Clients (Methoden, URI, Header, Status-Codes)	▸Kommunikationsszenario HKS.WS1.CLI: Nutzung von Webservices des SMGW mit Authentifizierung durch TLS-Client-Zertifikat
SOCKS-TLS	Anforderungen an den SOCKS-TLS-Client	▸HKS.TLSPROXY.SOCKSCLI
TLS	Anforderungen an den TLS-Handshake als TLS-Client	▸HKS.NTP-TLS.CLI, ▸Kommunikationsszenario HKS.WS1.CLI: Nutzung von Webservices des SMGW mit Authentifizierung durch TLS-Client-Zertifikat, ▸HKS.TLSPROXY.SOCKSCLI, ▸HKS.TLSPROXY.CLI
TLS	Anforderungen an den TLS-Handshake als TLS-Server	▸HKS.TLSPROXY.SRV
NTP	Anforderungen an den NTP-Client	▸HKS.NTP-TLS.CLI
mDNS	Anforderungen für das mDNS-Querying	▸HKS.DNSDISCOVERY

Tabelle 4.1 Mitgeltende Teile der Detailspezifikation

4.4 Interoperabilitätsvorgaben an die Schnittstelle zum HAN des SMGW

4.4.1 Einleitung

Dieser Abschnitt spezifiziert die Interoperabilitätsanforderungen an die Kommunikationsszenarien von CLS-Kommunikationsadaptern. Eine Übersicht über die Kommunikationsszenarien findet sich in ▸Tabelle 4.2.

Kommunikationsszenario	Beschreibung	Siehe Abschnitt	SMGW-Kommunikationsszenario
HKS.TLSPROXY.SOCKSCLI	Sicherer Austausch von Anwendungsinformationen eines CLS-Kommunikationsadapters mit einem Kommunikationspartner im WAN über einen durch das SMGW vermittelten TLS-Proxy-Kanal, der durch eine vom CLS-Kommunikationsadapter abgehende Verbindung zum SMGW an dessen HAN-Schnittstelle mittels SOCKS-TLS initiiert wird.	▸Abschnitt 4.4.4	HKS.TLSPROXY.SOCKS (HKS3)
HKS.TLSPROXY.CLI	Sicherer Austausch von Anwendungsinformationen eines CLS-Kommunikationsadapters mit einem Kommunikationspartner im WAN über einen durch das SMGW vermittelten TLS-Proxy-Kanal, der durch eine vom CLS-Kommunikationsadapter abgehende Verbindung zum SMGW an dessen HAN-Schnittstelle mittels TLS-ServerNameIndication initiiert wird.	▸Abschnitt 4.4.5	HKS.TLSPROXY.SRV (HKS3 mit TLS-SNI)

Kommunikationsszenario	Beschreibung	Siehe Abschnitt	SMGW-Kommunikationsszenario
HKS.TLSPROXY.SRV	Sicherer Austausch von Anwendungsinformationen eines CLS-Kommunikationsadapters mit einem Kommunikationspartner im WAN über einen durch das SMGW vermittelten TLS-Proxy-Kanal, der durch eine vom SMGW abgehende Verbindung zum CLS-Kommunikationsadapter initiiert wird.	▸Abschnitt 4.4.6	HKS.TLSPROXY.CLI (HKS4/HKS5)
HKS.DNSDISCOVERY	Auffinden eines SMGW durch einen CLS-Kommunikationsadapter.	▸Abschnitt 4.4.7	HKS.DNSDISCOVERY
HKS.NTP-TLS.CLI	Authentischer Zeitbezug vom SMGW mittels NTP über TLS.	▸Abschnitt 4.4.8	HKS.NTP-TLS.SRV
HKS.WS1.CLI	Zugriff auf Dienste des SMGW über RESTful Webservices mit Authentifizierung des CLS-Kommunikationsadapters durch TLS-Zertifikat	▸Abschnitt 4.4.9	HKS.WS1.SRV

Tabelle 4.2 Übersicht der Kommunikationsszenarien im HAN des SMGW

Ein HKS ist über das Tupel (TCP-Portnummer [, TLS-ServerNameIndication][, TLS-ClientZertifikat]) beim Verbindungsaufbau für den TLS-Server identifizierbar. Die Portnummer ist entweder über Standards definiert (well-known Port), im SMGW und CLS-Kommunikationsadapter vorkonfiguriert (z.B. über elektronischen Lieferschein) oder über DNS-SD (Siehe ▸Abschnitt 4.4.7) anhand eines standardisierten well-known Service-Names ermittelt worden.[1]

▸Abbildung 4.1 zeigt die Übersicht über den HAN-Protokollstapel.

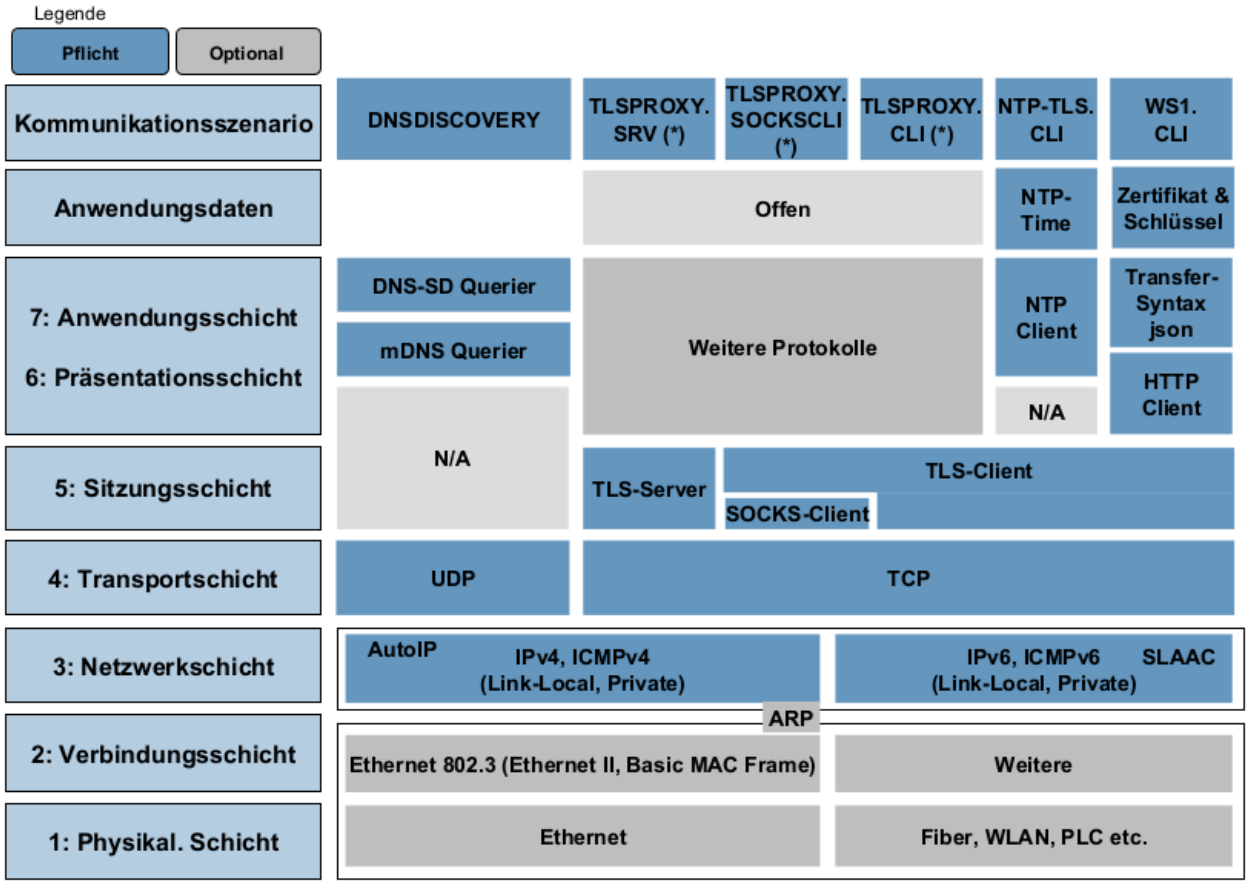

Abbildung 4.1. In dieser TR beschriebene Kommunikationsszenarien

[1] Siehe IANA "Service Name and Transport Protocol Port Number Registry" (https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml")

Anmerkung (*): Eine *TLS-Verbindung* wird entweder vom CLS-Kommunikationsadapter zum SMGW aufgebaut (Kommunikationsszenario ▸HKS.TLSPROXY.CLI oder ▸HKS.TLSPROXY.SOCKSCLI) oder vom SMGW zum CLS-Kommunikationsadapter (▸HKS.TLSPROXY.SRV). Der Hersteller entscheidet unter der Beachtung von ▸REQ.IOP.KS.HAN.30 und ▸REQ.IOP.KS.HAN.40, ob der CLS-Kommunikationsadapter sowohl abgehende als auch ankommende TLS-Proxy-Verbindungen oder nur eine der beiden Möglichkeiten unterstützt.

4.4.2 Sicherung der Kommunikation

REQ.IOP.KS.HAN.10

Um die Authentizität und Vertraulichkeit der Daten im TLS-Proxy-Kanal zu gewährleisten, **MUSS** der CLS-Kommunikationsadapter das SMGW authentifizieren und den TLS-Verbindungsaufbau beenden, sofern das vom Kommunikationspartner im HAN präsentierte TLS-Client Zertifikat

- (vom SMGW) selbstsigniert ist und nicht dem im CLS-Kommunikationsadapter persistierten GW_HAN_TLS_CRT entspricht, oder
- von einer CA ausgestellt wurde und nicht mit dem im CLS-Kommunikationsadapter persistierten Vertrauensanker (CA-Zertifikat) validiert werden kann, oder
- von einer SM-PKI-CA ausgestellt wurde und nicht die Funktion "smgw" hat.

Ausnahmsweise kann im Rahmen der initialen kommunikativen Anbindung auf die Authentifizierung des SMGW mittels Zertifikat verzichtet werden, solange kein Vertrauensanker zur Validierung des TLS-Zertifikates des SMGW im CLS-Kommunikationsadapter persistiert ist und gewährleistet ist, dass das TLS-Zertifikat des SMGW unverändert zum CLS-Kommunikationsadapter übermittelt wird.

Der CLS-Kommunikationsadapter **MUSS** sich gegenüber dem SMGW mit seinem CLS_HAN_TLS_CRT authentisieren. [REQ.IOP.KS.HAN.20]

4.4.3 Kommunikationsprotokolle

Der CLS-Kommunikationsadapter **MUSS** ▸HKS.TLSPROXY.SRV oder ▸HKS.TLSPROXY.SOCKSCLI zur Kommunikation mit dem SMGW nutzen können. [REQ.IOP.KS.HAN.30]

Nutzt der CLS-Kommunikationsadapter ▸HKS.TLSPROXY.SOCKSCLI, so **MUSS** er ▸HKS.TLSPROXY.CLI zur Kommunikation mit dem SMGW nutzen können. [REQ.IOP.KS.HAN.40]

Der CLS-Kommunikationsadapter **MUSS** *IPv4* und *ICMPv4* als Netzwerkprotokoll im HAN des SMGW unterstützen. [REQ.IOP.KS.HAN.50]

Der CLS-Kommunikationsadapter **MUSS** *IPv6* und *ICMPv6* als Netzwerkprotokoll im HAN des SMGW unterstützen. [REQ.IOP.KS.HAN.60]

Der CLS-Kommunikationsadapter **MUSS** ausschließlich link-lokale oder private (nicht-routbare) Quell- und Zieladressen des IP-Netzwerkprotokolls im HAN des SMGW unterstützen (statisch oder dynamisch konfiguriert). [REQ.IOP.KS.HAN.70]

Der CLS-Kommunikationsadapter **MUSS** die dynamische Adressvergabe link-lokaler IPv4-Adressen ("Zero-Configuration") im HAN des SMGW unterstützen. [REQ.IOP.KS.HAN.80]

Der CLS-Kommunikationsadapter **MUSS** die dynamische Adressvergabe für link-lokale IPv6-Adressen (SLAAC) im HAN des SMGW unterstützen. [REQ.IOP.KS.HAN.90]

Der CLS-Kommunikationsadapter **MUSS** das Kommunikationsszenario HKS.DNSDISCOVERY umsetzen. [REQ.IOP.KS.HAN.100]

Der CLS-Kommunikationsadapter **MUSS** das Kommunikationsszenario HKS.NTP-TLS.CLI umsetzen. [REQ.IOP.KS.HAN.110]

Der CLS-Kommunikationsadapter **MUSS** das Kommunikationsszenario HKS.WS1.CLI umsetzen. [REQ.IOP.KS.HAN.120]

ICS

ICS.IOP.HKS.TLSPROXY.10

Der Hersteller **MUSS** im ICS deklarieren, ob der CLS-Kommunikationsadapter eingehende TLS-Proxy-Verbindungen via ▸HKS.TLSPROXY.SRV zur Kommunikation mit dem SMGW unterstützt.

ICS.IOP.HKS.TLSPROXY.20

Der Hersteller **MUSS** im ICS deklarieren, ob der CLS-Kommunikationsadapter ausgehende TLS-Proxy-Verbindungen via ▸HKS.TLSPROXY.SOCKSCLI zur Kommunikation mit dem SMGW unterstützt.

4.4.4 HKS.TLSPROXY.SOCKSCLI

4.4.4.1 Beschreibung

Das HKS.TLSPROXY.SOCKSCLI fasst die Protokolle und Nachrichtenformate zusammen, über die CLS-Kommunikationsadapter an ihrer Schnittstelle zum HAN des SMGW *TLS-Verbindungen* über die TLS-Proxy-Funktion des SMGW zu einem Kommunikationspartner im WAN nutzen können. Die Signalisierung der *ProxyId* des Kommunikationspartners im WAN, zu dem die Verbindung aufgebaut werden soll, erfolgt über das SOCKS-Protokoll mit Authentifizierung und Transportsicherung durch das TLS-Protokoll.

Um authentisch und vertraulich Daten mit Kommunikationspartnern im WAN auszutauschen, kann der CLS-Kommunikationsadapter Kommunikationskanäle über die TLS-Proxy-Funktion des SMGW initiieren. Dazu signalisiert die Implementierung beim TLS-Verbindungsaufbau authentisch einen Bezeichner an das SMGW (*ProxyId*). Basierend auf dem authentisch übermittelten Zertifikat des CLS-Kommunikationsadapters und der *ProxyId* ermittelt das SMGW das konfigurierte Verbindungsziel des TLS-Proxy-Kanals, zu dem das SMGW eine Verbindung herstellt. Dieses Kapitel beschreibt die Mindestanforderungen an die Protokolle zur Verwendung des TLS-Proxy-Kanals, wenn die Implementierung den TLS-Proxy-Kanal als TLS-Client zum SMGW initiiert.

Dieses KS besteht aus den folgenden Protokollen:

- Verbindungsorientiertes Transportprotokoll TCP mit abgehenden Verbindungen, um eine zuverlässige und interoperable Transportverbindung zwischen einem SMGW und CLS-Kommunikationsadapter herzustellen.
- TLS für den CLS-Kommunikationsadapter in der Rolle des Clients, um vertrauliche und authentische Transportverbindungen zwischen CLS-Kommunikationsadapter und dem SMGW zu gewährleisten.
- Signalisierung der TLS-Proxy-Verbindung mit SOCKS gemäß Detailspezifikation SOCKS-TLS für den CLS-Kommunikationsadapter in der Rolle des Clients.
- (Anwendungs-)Nachrichten, die vom TLS-Protokoll transportiert werden, an die durch diese TR keine Interoperabilitätsanforderungen gestellt werden.

▸Abbildung 4.2 und ▸Abbildung 4.3 verdeutlichen den Ablauf eines durch den SOCKS-Client initiierten TLS-Proxy-Kanals.

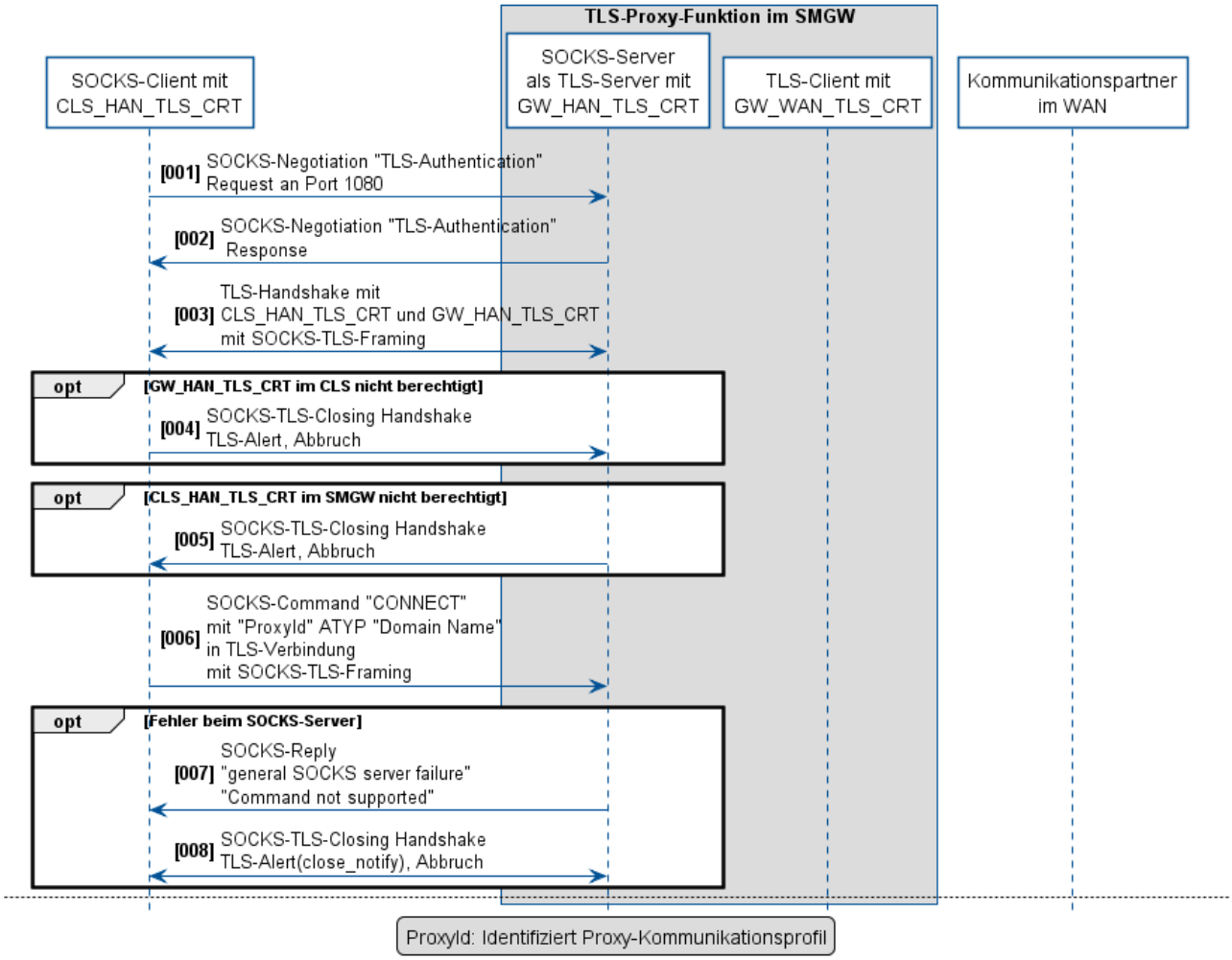

Abbildung 4.2. Übersicht über den Ablauf bei der Verwendung eines SOCKS-TLS-Proxy-Kanals (1/2)

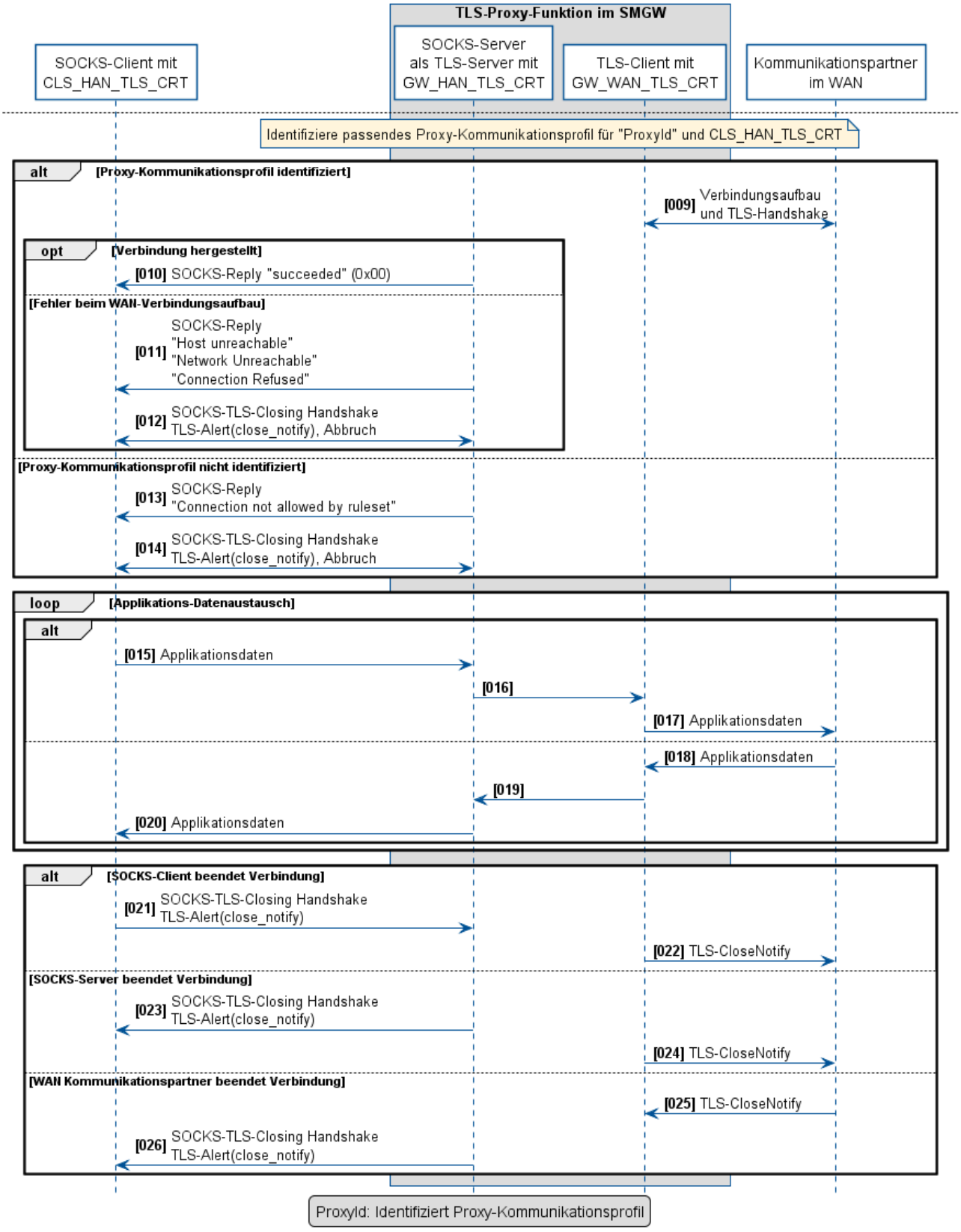

Abbildung 4.3. Übersicht über den Ablauf bei der Verwendung eines SOCKS-TLS-Proxy-Kanals (2/2)

Abbildung 4.4 verdeutlicht den Protokollstack und die Schachtelung der Nachrichten.

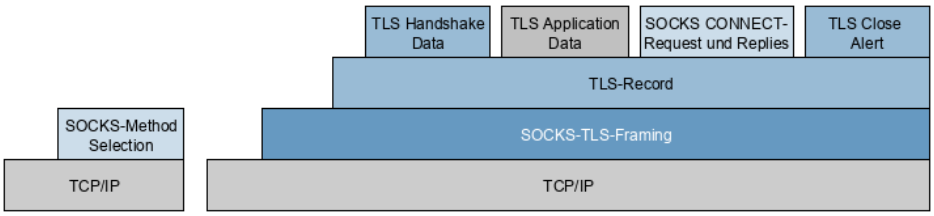

Abbildung 4.4. Übersicht über die Nachrichtenschachtelung des HKS.TLSPROXY.SOCKSCLI

4.4.4.2 Vorbedingungen

- Die IP-Adresse des SMGW und die Portnummer für die Verbindung zum SOCKS-TLS Service des SMGW liegen vor (Siehe ▸HKS.DNSDISCOVERY).
- Die ProxyId, d.h. die in der SOCKS CONNECT-Nachricht übermittelte Identifikation zur Auswahl des TLS-Proxy-Kanals zum Kommunikationspartner im WAN liegt vor.
- Das für die Validierung des präsentierten TLS-Server-Zertifikates verwendete CA-Zertifikat bzw. selbstsignierte GW_HAN_TLS_CRT liegt im CLS-Kommunikationsadapter vor.

4.4.4.3 Sicherung der Kommunikation

Siehe ▸Abschnitt 4.4.2.

4.4.4.4 Kommunikationsprotokolle

Der CLS-Kommunikationsadapter **MUSS** TCP gemäß [RFC9293] in der Rolle des Initiators (active open) implementieren. [REQ.HKS.TLSPROXY.SOCKSCLI.20]

Der CLS-Kommunikationsadapter **MUSS** TLS gemäß Detailspezifikation [DS] Kapitel TLS in der Rolle des TLS-Clients implementieren. [REQ.HKS.TLSPROXY.SOCKSCLI.30]

An die Struktur der Anwendungsdaten werden keine Vorgaben gemacht.

4.4.4.5 Technische Anwendungsfälle

Das Kommunikationsszenario HKS.TLSPROXY.SOCKSCLI verwendet folgende technische Anwendungsfälle deren Detailanforderungen in [DS]) beschrieben sind:

- Aktives Öffnen einer TCP-Verbindung (abgehende Verbindung)
- Öffnen einer TLS-Session als Client
- Empfangen von TLS-Applikationsdaten
- Senden von TLS-Applikationsdaten
- Schließen der TCP/TLS-Verbindung nach Empfang eines CloseNotify Alerts
- Schließen der TCP/TLS-Verbindung, initiiert durch den CLS-Kommunikationsadapter

In der Default-Konfiguration **MUSS** der CLS-Kommunikationsadapter den TCP-Port 1080 (SOCKS) für abgehende Verbindungen verwenden. [REQ.HKS.TLSPROXY.SOCKSCLI.40]

4.4.5 HKS.TLSPROXY.CLI

4.4.5.1 Beschreibung

Das HKS.TLSPROXY.CLI fasst die Protokolle und Nachrichtenformate zusammen, über die ein CLS-Kommunikationsadapter an seiner Schnittstelle zum SMGW eine *TLS-Verbindung* über das SMGW zu einem Kommunikationspartner im WAN aufbauen kann. Die Signalisierung der *ProxyId* des Kommunikationspartners im WAN, zu dem die Verbindung aufgebaut werden soll, erfolgt über die *ServerNameIndication* im TLS-Handshake-Protokoll.

Um authentisch und vertraulich Daten mit Kommunikationspartnern im WAN auszutauschen, kann ein CLS-Kommunikationsadapter Kommunikationskanäle über die TLS-Proxy-Funktion des SMGW initiieren. Dazu

signalisiert die Implementierung beim TLS-Verbindungsaufbau authentisch einen Bezeichner an das SMGW (*ProxyId*). Basierend auf dem authentisch übermittelten Zertifikat des CLS-Kommunikationsadapters und der *ProxyId* ermittelt das SMGW das konfigurierte Verbindungsziel des TLS-Proxy-Kanals, zu dem das SMGW eine Verbindung herstellt.

Diese KS besteht aus den folgenden Protokollen:

- Verbindungsorientiertes Transportprotokoll TCP mit abgehenden Verbindungen, um eine zuverlässige und interoperable Transportverbindung zwischen einem SMGW und CLS-Kommunikationsadapter herzustellen
- TLS für den CLS-Kommunikationsadapter in der Rolle des Clients, um vertrauliche und authentische Transportverbindungen zwischen CLS-Kommunikationsadapter und SMGW zu gewährleisten.
- (Anwendungs-)Nachrichten, die über das TLS-Protokoll transportiert werden, an die keine Interoperabilitätsanforderungen gestellt werden.

▸Abbildung 4.5 verdeutlicht den Ablauf eines durch den CLS-Kommunikationsadapter initiierten TLS-Proxy-Kanals.

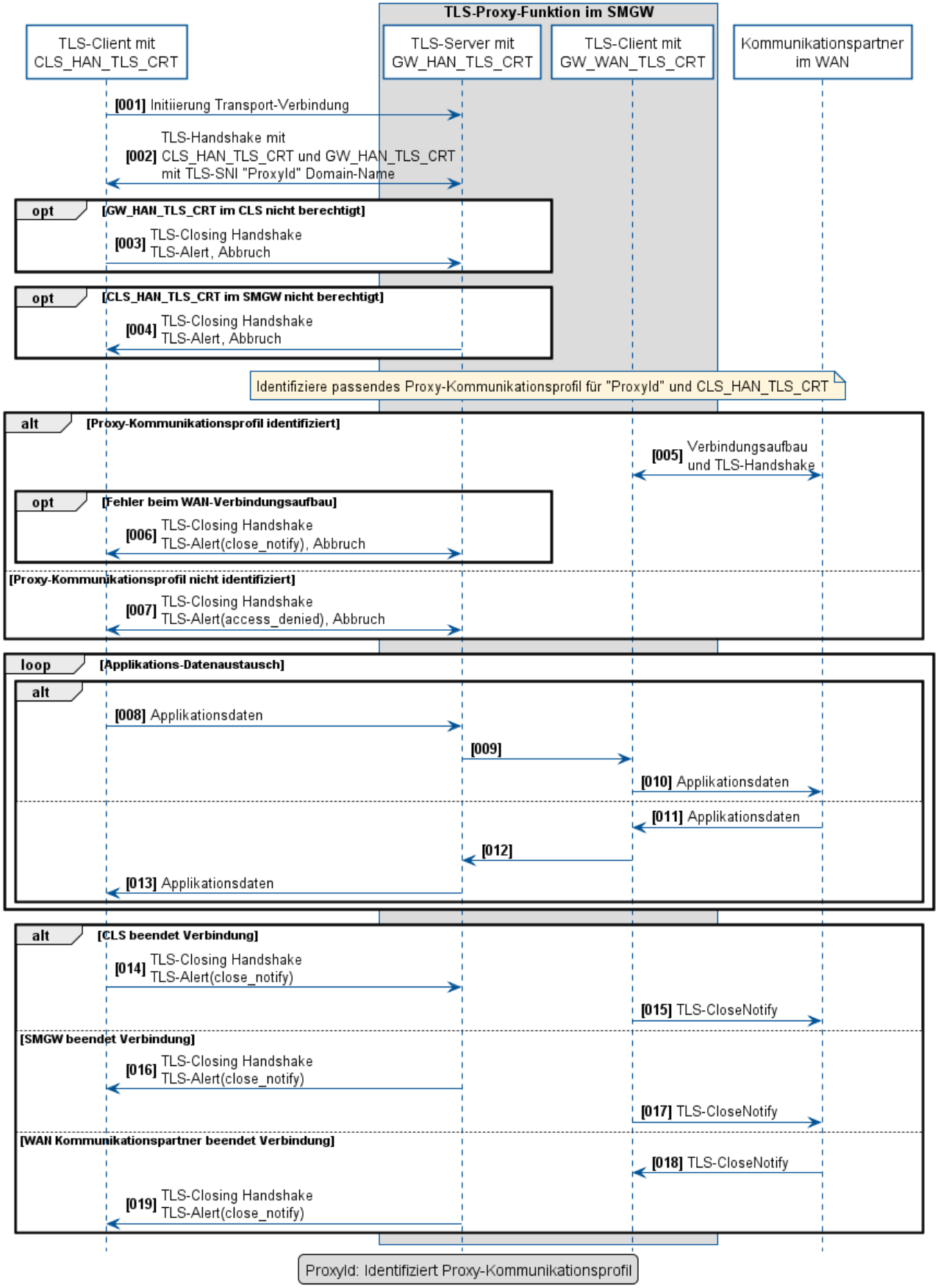

Abbildung 4.5. Übersicht über den Ablauf bei der Verwendung eines durch den CLS-Kommunikationsadapter initiierten TLS-Proxy-Kanals

4.4.5.2 Vorbedingungen

- Die IP-Adresse des SMGW und die Portnummer für die Verbindung zum TLS-Service des SMGW liegen vor (Siehe ▸HKS.DNSDISCOVERY).
- Die *ProxyId*, d.h. die im TLS-SNI übermittelte Identifikation zur Auswahl des TLS-Proxy-Kanals zum Kommunikationspartner im WAN liegt vor.
- Das für die Validierung des präsentierten TLS-Server-Zertifikates verwendete CA-Zertifikat bzw. selbstsignierte GW_HAN_TLS_CRT liegt im CLS-Kommunikationsadapter vor.

4.4.5.3 Sicherung der Kommunikation

Siehe ▸Abschnitt 4.4.2.

4.4.5.4 Kommunikationsprotokolle

Der CLS-Kommunikationsadapter **MUSS** TCP gemäß [RFC9293] in der Rolle des Initiators (active open) implementieren. [REQ.HKS.TLSPROXY.CLI.20]

Der CLS-Kommunikationsadapter **MUSS** TLS gemäß Detailspezifikation [DS] Kapitel TLS in der Rolle des TLS-Clients implementieren. [REQ.HKS.TLSPROXY.CLI.30]

Der CLS-Kommunikationsadapter **MUSS** die ProxyId im Namensfeld der ClientHello-Extension server_name gemäß [RFC6066] übermitteln. Die Zeichen sind als DNS-Name gemäß [RFC1035] auf a-z, Bindestrich, Punkt und 0-9 beschränkt und der server_name darf nicht leer sein. Der server_name soll nicht länger als 63 Zeichen sein. [REQ.HKS.TLSPROXY.CLI.40]

An die Struktur der Anwendungsdaten werden keine Vorgaben gemacht.

4.4.5.5 Technische Anwendungsfälle

Das Kommunikationsszenario HKS.TLSPROXY.CLI verwendet folgende technische Anwendungsfälle deren Detailanforderungen in [DS]) beschrieben sind:

- Aktives Öffnen einer TCP-Verbindung
- Öffnen einer TLS-Session als Client
- Empfangen von TLS-Applikationsdaten
- Senden von TLS-Applikationsdaten
- Schließen der TCP/TLS-Verbindung nach Empfang eines CloseNotify Alerts
- Schließen der TCP/TLS-Verbindung, initiiert durch den CLS-Kommunikationsadapter

ICS.HKS.TLSPROXY.CLI.10

Der Hersteller **MUSS** im ICS deklarieren, welchen Destination-Port der CLS-Kommunikationsadapter bei abgehenden HKS.TLSPROXY.CLI Verbindungen in der Default-Konfiguration für die Zieladresse des SMGW verwendet.

Der Port identifiziert in der Regel das Applikationsprotokoll.[2]

4.4.6 HKS.TLSPROXY.SRV

4.4.6.1 Beschreibung

Das HKS.TLSPROXY.SRV fasst die Protokolle und Nachrichtenformate zusammen, über die ein CLS-Kommunikationsadapter an seiner Schnittstelle zum SMGW einen Dienst anbietet, damit ein SMGW einen TLS-Proxy-Kanal von einem Kommunikationspartner im WAN zum CLS-Kommunikationsadapter aufbauen kann.[3]

Dieses KS besteht aus den folgenden Protokollen:

[2] Beispiele: https: Port 443, websocket over TLS: Port 443, xmpp over TLS: 5223, mqtt over TLS: 8883

[3] In TR-03109-1v1.1 ist das SMGW-seitige HKS mit HKS4 und HKS5 bezeichnet.

- Verbindungsorientiertes Transportprotokoll TCP mit ankommenden Verbindungen, um eine zuverlässige und interoperable Transportverbindung zwischen einem SMGW und CLS-Kommunikationsadapter herzustellen.
- TLS für den CLS-Kommunikationsadapter in der Rolle des Servers, um vertrauliche und authentische Transportverbindungen zwischen CLS-Kommunikationsadapter und SMGW zu gewährleisten.
- (Anwendungs-)Nachrichten, die vom TLS-Protokoll transportiert werden, an die keine Interoperabilitätsanforderungen gestellt werden.

▸Abbildung 4.6 verdeutlicht den Ablauf eines durch das SMGW initiierten TLS-Proxy-Kanals.

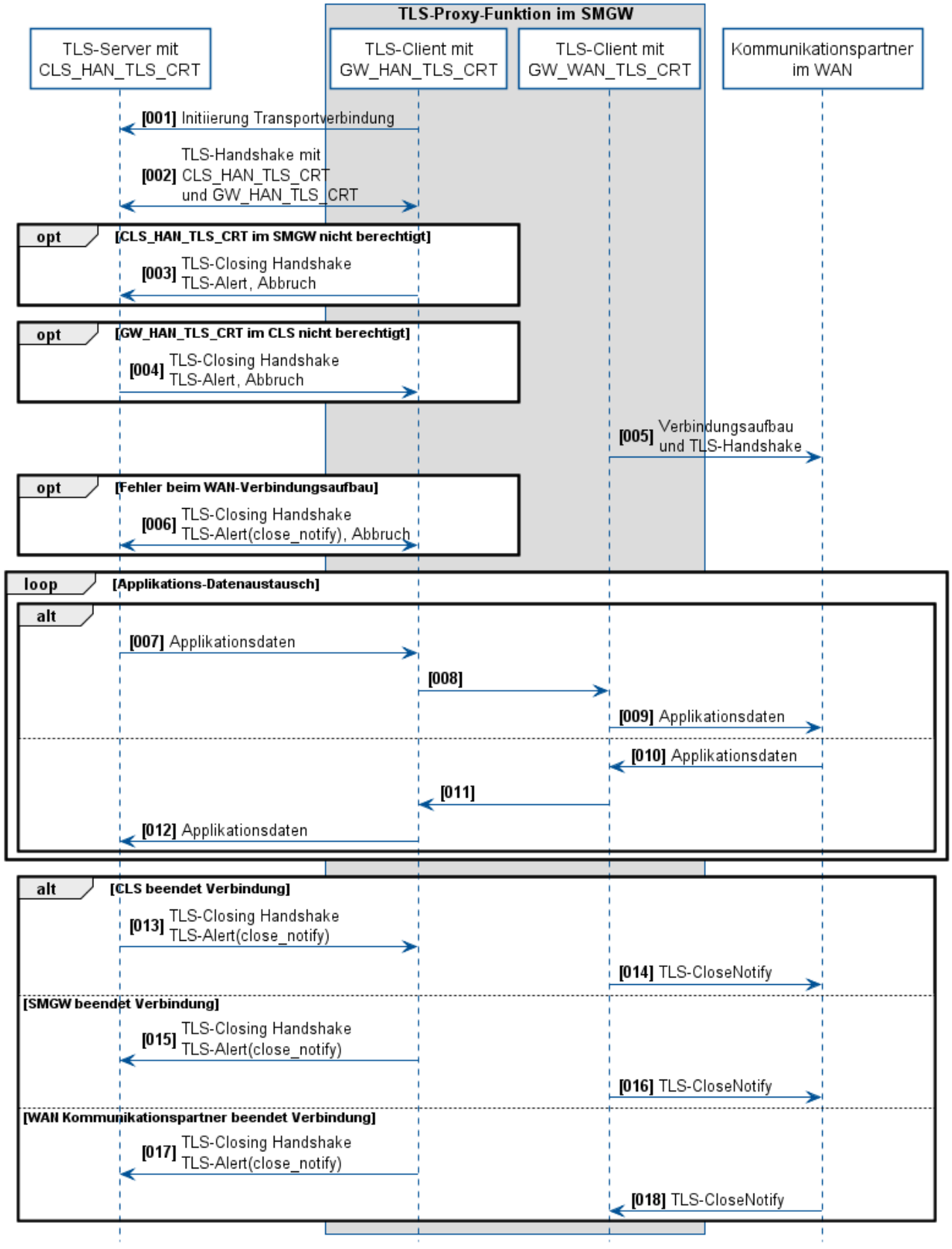

Abbildung 4.6. Übersicht über den Ablauf bei der Verwendung eines durch das SMGW initiierten TLS-Proxy-Kanals

4.4.6.2 Vorbedingungen

- Im SMGW liegen die IP-Adresse und die Portnummer für die Verbindung zum TLSPROXY-SRV des CLS-Kommunikationsadapters vor

- Das für die Validierung des präsentierten TLS-Client-Zertifikates verwendete CA-Zertifikat (bzw. selbstsignierte GW_HAN_TLS_CRT) liegt im CLS-Kommunikationsadapter vor.
- Das CLS_HAN_TLS_CRT des CLS-Kommunikationsadapters liegt im SMGW vor.

4.4.6.3 Sicherung der Kommunikation

Siehe ▸Abschnitt 4.4.2.

4.4.6.4 Kommunikationsprotokolle

Der CLS-Kommunikationsadapter **MUSS** TCP gemäß [RFC9293] in der Rolle des Acceptors (passive open) implementieren. [REQ.HKS.TLSPROXY.SRV.20]

Der CLS-Kommunikationsadapter **MUSS** TLS gemäß Detailspezifikation [DS] Kapitel TLS in der Rolle des TLS-Servers implementieren. [REQ.HKS.TLSPROXY.SRV.30]

An die Struktur der Anwendungsdaten werden keine Vorgaben gemacht.

4.4.6.5 Technische Anwendungsfälle

Das Kommunikationsszenario HKS.TLSPROXY.SRV verwendet folgende technische Anwendungsfälle deren Detailanforderungen in [DS]) beschrieben sind:

- Passives Öffnen einer TCP-Verbindung (Ankommende Verbindung)
- Öffnen einer TLS-Session als Server
- Empfangen von TLS-Applikationsdaten
- Senden von TLS-Applikationsdaten
- Schließen der TCP/TLS-Verbindung nach Empfang eines CloseNotify Alerts
- Schließen der TCP/TLS-Verbindung, initiiert durch den CLS-Kommunikationsadapter

ICS.HKS.TLSPROXY.SRV.10

Der Hersteller **MUSS** im ICS deklarieren, welchen Default-Port der CLS-Kommunikationsadapter bei ankommenden HKS.TLSPROXY.SRV Verbindungen verwendet.

Der Port identifiziert in der Regel das Applikationsprotokoll.[4]

4.4.7 HKS.DNSDISCOVERY

4.4.7.1 Beschreibung

Das HKS.DNSDISCOVERY unterstützt die interoperable und automatische Feststellung einer Geräte- oder Dienstadresse mittels DNS im HAN des SMGW.

Das SMGW bietet Entitäten in seinem HAN (z.B. berechtigten lokalen Nutzern, dem Service-Techniker des SMGW, CLS-Kommunikationsadaptern) Dienste an seiner HAN-Schnittstelle an. Ein CLS-Kommunikationsadapter muss zum Aufruf eines FA über ein HAN Kommunikationsszenario Kenntnis über die Link-, Netzwerk- und Transportadresse des für den Dienst zuständigen SMGW erhalten, bevor eine TLS-Verbindung vom CLS-Kommunikationsadapter zum SMGW aufgebaut werden kann. Dies kann durch vorherige Konfiguration (statische Vereinbarung) oder automatisch (dynamische Vereinbarung) geschehen. Die folgenden Abschnitte beschreiben den Ablauf und die Anforderungen zum automatischen Ermitteln der Netzwerk- und Dienstadressen des SMGW. Da dies ohne vorherige Konfiguration des CLS-Kommunikationsadapters geschieht, wird das Verfahren auch als "Zero-Configuration" bezeichnet.

Dieses KS besteht aus den folgenden Protokollen:

[4] Beispiele: http, websocket: Port 443, xmpp: 5223, mqtt: 8883

- Der CLS-Kommunikationsadapter verwendet UDP/IP mit Multicast zum Transport der mDNS und DNS-SD Nachrichten, sowie Link-, Netzwerk- und Transportprotokoll in der Rolle des *Acceptors* und *Originators*, um den verbindungslosen Transport im Netzwerk zum SMGW herzustellen.
- Optional kann der CLS-Kommunikationsadapter mDNS/DNS-SD über UDP/IPv6 implementieren.
- Der CLS-Kommunikationsadapter verwendet an seiner Schnittstelle zum SMGW das link-lokale mDNS Querying, so dass der CLS-Kommunikationsadapter die Netzwerkadresse zu einer bekannten *SMGW-ID* erhalten kann, bzw. die Netzwerkadressen von SMGW erfragen kann. Sofern das SMGW einen mDNS Responder Dienst gemäß [DS] unterstützt, werden mDNS-Adressanfragen nach "<SMGW-ID>.local." und "smgw.local." mit der link-lokalen oder privaten Netzwerkadresse des SMGW beantwortet.
- Optional kann der CLS-Kommunikationsadapter DNS-Service Discovery (DNS-SD) gemäß [RFC6763] implementieren, um die TCP-Port-Nummern für die Diensttypen ("serviceTypes") des SMGW auf Anfrage zu erhalten.

Abbildung 4.7 verdeutlicht den Ablauf der Adressbestimmung über mDNS/DNS-SD.

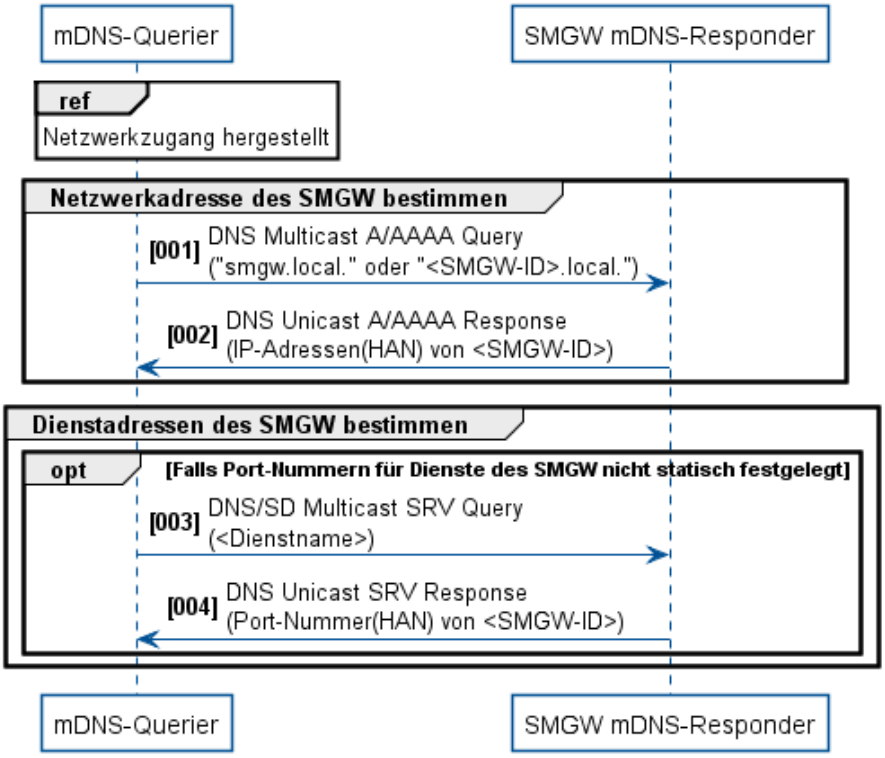

Abbildung 4.7. Übersicht über den Ablauf der automatischen Adressbestimmung im HAN

4.4.7.2 Vorbedingungen

Der CLS-Kommunikationsadapter und das SMGW befinden sich im gleichen Netzwerk.

4.4.7.3 Kommunikationsprotokolle

Der CLS-Kommunikationsadapter **MUSS** die IPv4-Adresse eines SMGW als mDNS-Querier gemäß [RFC6762] bestimmen können. [REQ.HKS.DNSDISCOVERY.10] Der CLS-Kommunikationsadapter **MUSS** die IPv6-Adresse eines SMGW als mDNS-Querier gemäß [RFC6762] bestimmen. [REQ.HKS.DNSDISCOVERY.20]

Sofern mDNS-Queries nach einem SMGW erfolgen, **MUSS** der CLS-Kommunikationsadapter den DNS-Host-Namen "smgw.local." verwenden können. [REQ.HKS.DNSDISCOVERY.30] Sofern mDNS-Queries nach einem individuellen SMGW erfolgen, **MUSS** der CLS-Kommunikationsadapter den DNS Host-Namen "<SMGW-ID>.local." verwenden können, wobei die SMGW-ID gemäß [DIN43849] gebildet wird. [REQ.HKS.DNSDISCOVERY.40]

Der CLS-Kommunikationsadapter **SOLL** die Dienstadressen (TCP-Ports) eines SMGW als mDNS-Querier mit DNS-SD gemäß [RFC6763] bestimmen. [REQ.IOP.HKS.DNSDISCOVERY.50]

ICS.HKS.DNSDISCOVERY.20

Der Hersteller **MUSS** im ICS deklarieren, ob DNS-SD nach [RFC6763] implementiert ist.

ICS.HKS.DNSDISCOVERY.30

Sofern ein DNS-SD-Querier implementiert ist **MUSS** der Hersteller im ICS die Abweichungen von den Anforderungen an den DNS-SD-Querier gemäß [RFC6763] beschreiben.

4.4.7.4 Technische Anwendungsfälle

Das Kommunikationsszenario HKS.DNSDISCOVERY verwendet folgende technische Anwendungsfälle deren Detailanforderungen in [DS]) beschrieben sind:

- Anfrage der IP-Adresse eines Hosts als mDNS-Querier
- Verarbeiten einer mDNS-Antwort nach einer IP-Adresse
- Anfrage einer Dienstadresse (Port) mittels DNS-SD anhand des Dienstnamens (optional)
- Verarbeiten einer DNS-SD Antwort nach einer Dienstadresse (Port) (optional)

4.4.8 HKS.NTP-TLS.CLI

4.4.8.1 Beschreibung

Das HKS.NTP-TLS.CLI fasst die Protokolle und Nachrichtenformate für eine Zeitsynchronisation mittels NTP bzw. SNTP über TLS zusammen, über die ein CLS-Kommunikationsadapter die Zeit vom SMGW bezieht.

Dieses KS besteht aus folgenden Protokollen:

- Verbindungsorientiertes Transportprotokoll TCP mit abgehenden Verbindungen
- TLS für den CLS-Kommunikationsadapter in der Rolle des Clients, um vertrauliche und authentische Transportverbindungen zwischen CLS-Kommunikationsadapter und SMGW zu gewährleisten
- NTP für den CLS-Kommunikationsadapter in der Rolle des Clients, um die Nachrichten zur Zeitsynchronisation auszutauschen

▸Abbildung 4.8 verdeutlicht den Nachrichtenaustausch zwischen CLS-Kommunikationsadapter und SMGW.

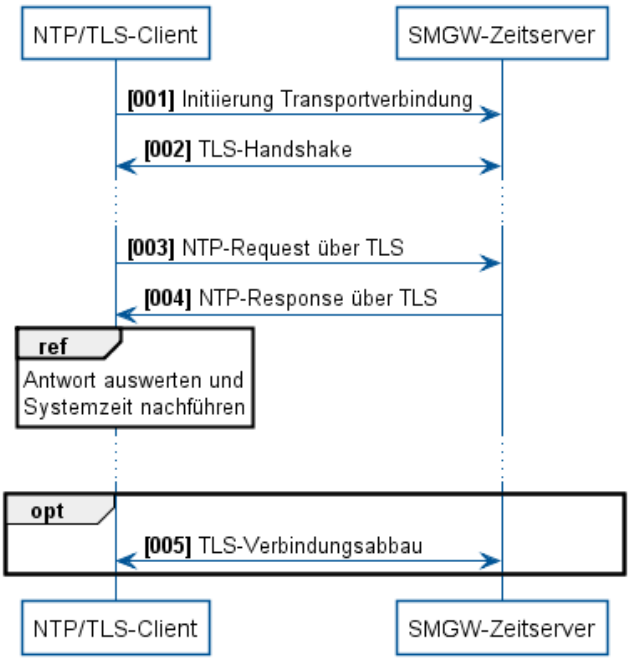

Abbildung 4.8. Übersicht über den Ablauf des HKS.NTP-TLS.CLI

Abbildung 4.9 verdeutlicht den Protokollstack und die Schachtelung der Nachrichten.

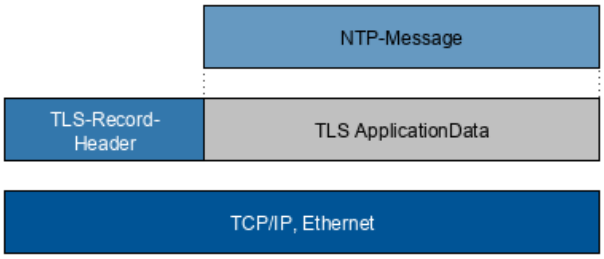

Abbildung 4.9. Übersicht über die Nachrichtenschachtelung des HKS.NTP-TLS.CLI

Der CLS-Kommunikationsadapter nutzt den Zeitserver des SMGW über NTP über TLS. Da eine 1:1 Zuordnung von NTP-Message und TLS-Application-Record vorliegt und darüber hinaus die NTP-Nachrichten eine feste Länge haben, ist kein Adaptionslayer zwischen NTP und TLS notwendig.

4.4.8.2 Vorbedingungen

- Die IP-Adresse des SMGW und die Portnummer für die Verbindung zum NTP-TLS Service des SMGW liegen vor (Siehe HKS.DNSDISCOVERY).
- Das für die Validierung des präsentierten TLS-Server-Zertifikates verwendete CA-Zertifikat bzw. selbstsignierte GW_HAN_TLS_CRT liegt im CLS-Kommunikationsadapter vor.

4.4.8.3 Sicherung der Kommunikation

Siehe Abschnitt 4.4.2.

4.4.8.4 Kommunikationsprotokolle

Der CLS-Kommunikationsadapter **MUSS** TCP gemäß [RFC9293] in der Rolle des Initiators (active open) verwenden. [REQ.HKS.NTP-TLS.20]

Der CLS-Kommunikationsadapter **MUSS** TLS gemäß Detailspezifikation [DS] Kapitel TLS in der Rolle des TLS-Clients verwenden. [REQ.HKS.NTP-TLS.30]

Der CLS-Kommunikationsadapter **MUSS** NTP gemäß Detailspezifikation [DS] Kapitel NTP in der Rolle des NTP-Clients verwenden. [REQ.HKS.NTP-TLS.40]

Der CLS-Kommunikationsadapter **MUSS** NTP-Request und NTP-Response ohne weitere Rahmeninformationen direkt in TLS-Application-Records übertragen. [REQ.HKS.NTP-TLS.50]

4.4.8.5 Technische Anwendungsfälle

Das Kommunikationsszenario verwendet folgende technische Anwendungsfälle deren Detailanforderungen in [DS]) beschrieben sind:

- Aktives Öffnen einer TCP-Verbindung (Initiieren)
- Öffnen einer TLS-Session als Client
- Erzeugen eines (S)NTP-Requests
- Verarbeiten einer (S)NTP-Response und nachführen der Systemzeit
- Schließen der TCP/TLS-Verbindung nach Empfang eines CloseNotify Alerts
- Schließen der TCP/TLS-Verbindung, initiiert durch den CLS-Kommunikationsadapter

In der Default-Konfiguration **MUSS** der CLS-Kommunikationsadapter den TCP-Port 4460 (NTS-KE) für den NTP-TLS-Service verwenden. [REQ.HKS.NTP-TLS.60]

Der CLS-Kommunikationsadapter **MUSS** im TLS-Handshake die Extension "Application Layer Protocol Negotiation" mit alpn = "ntp/4" senden. [REQ.HKS.NTP-TLS.70]

4.4.9 Kommunikationsszenario HKS.WS1.CLI: Nutzung von Webservices des SMGW mit Authentifizierung durch TLS-Client-Zertifikat

4.4.9.1 Beschreibung

Das HKS.WS1 fasst die Protokolle und Nachrichtenformate zusammen, über die der CLS-Kommunikationsadapter HAN-Webservices des SMGW nutzt. Der CLS-Kommunikationsadapter identifiziert und authentifiziert sich gegenüber dem SMGW mit seinem TLS-Zertifikat.

Dieses KS besteht aus folgenden Protokollen:

- Verbindungsorientiertes Transportprotokoll TCP mit vom CLS-Kommunikationsadapter abgehenden Verbindungen
- TLS in der Rolle des Clients, um vertrauliche und authentische Transportverbindungen zwischen CLS-Kommunikationsadapter und SMGW zu gewährleisten
- HTTP mit RESTful Webservices in der Rolle des Clients

Der CLS-Kommunikationsadapter verwendet im TLS-Handshake das geräteindividuelle CLS_HAN_TLS_CRT gemäß [DS] Kapitel "HAN-Zertifikatsprofile".

Das SMGW bietet die Webservice-API vorzugsweise auf Port 443 (https) an. Dem Webservice-Zugriff über HTTP liegt das REST-Konzept zugrunde, bei dem ein uniformer (kleiner) Satz von Zugriffs-Verben auf verschiedene Ressourcen angewandt werden kann. Die Ressourcen können jeweils von unterschiedlichem Inhaltstyp (Content-Type) sein. Darüber hinaus bietet das SMGW Dienste zum Aufruf von Funktionen über das Webservice-API an.

▸Abbildung 4.10 verdeutlicht den Ablauf des HKS.WS1.

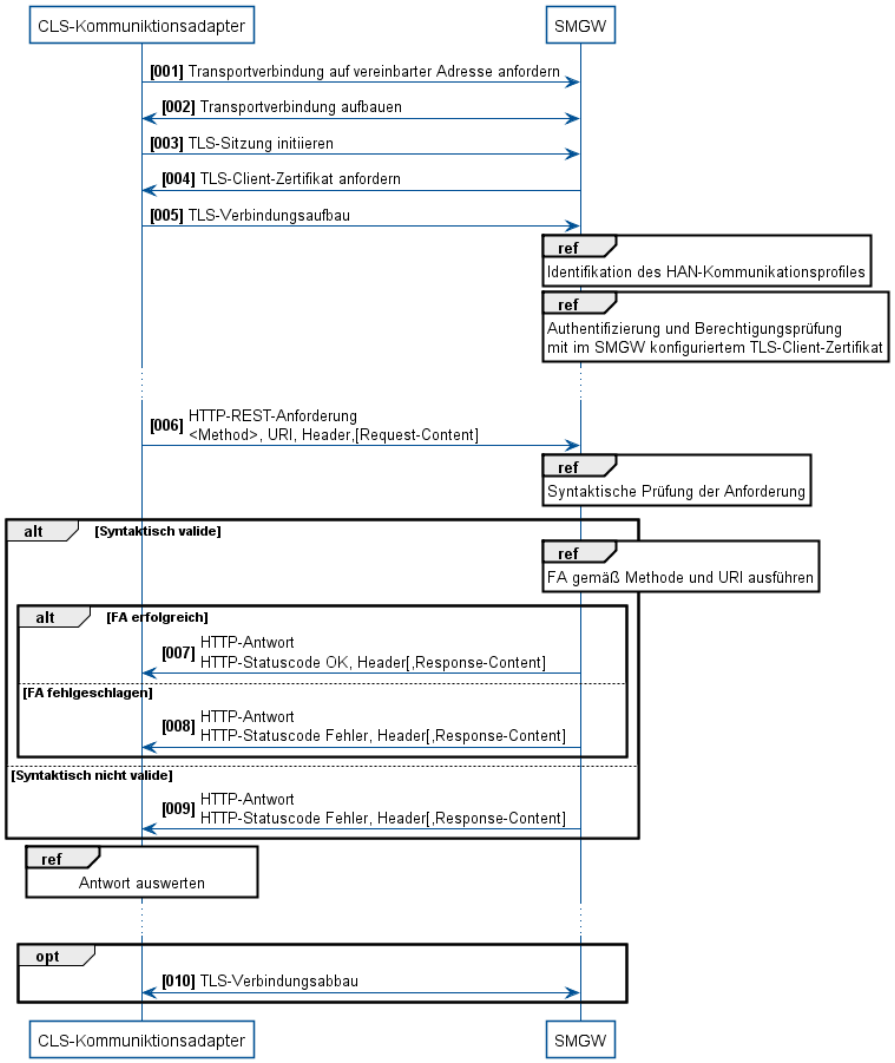

Abbildung 4.10. Authentifizierung des Nutzers im HAN mittels TLS-Client-Zertifikat

4.4.9.2 Vorbedingungen

- Die IP-Adresse des SMGW und die Portnummer für die Verbindung zum NTP-TLS Service des SMGW liegen vor (Siehe ▸HKS.DNSDISCOVERY).
- Das für die Validierung des präsentierten TLS-Server-Zertifikates verwendete CA-Zertifikat bzw. selbstsignierte GW_HAN_TLS_CRT liegt im CLS-Kommunikationsadapter vor.

4.4.9.3 Sicherung der Kommunikation

Siehe ▸Abschnitt 4.4.2.

4.4.9.4 Kommunikationsprotokolle

Der CLS-Kommunikationsadapter **MUSS** TCP gemäß [RFC9293] in der Rolle des Initiators (active open) verwenden. [REQ.HKS.WS1.CLI.20]

Der CLS-Kommunikationsadapter **MUSS** TLS gemäß Detailspezifikation [DS] Kapitel TLS in der Rolle des TLS-Clients verwenden. [REQ.HKS.WS1.CLI.30]

Der CLS-Kommunikationsadapter **MUSS** den Zugriff auf Ressourcen des SMGW über das Kommunikationsszenario HKS.WS1 mit einem RESTful Webservice Protokoll gemäß [DS] "RESTful Webservice" als HTTP-Client unterstützen. [REQ.HKS1.WS1.CLI.40]

> Gemäß [TR-03109-1] wird der Dienstaufruf zur Erzeugung von CLS-Schlüsselpaar und -Zertifikat mit einem HTTP-Request "POST /smgw/cls/v1/fas/CreateKeyPairAndCert" durchgeführt, worauf das SMGW

eine HTTP-Response mit dem Content-Type "application/json" liefert, in dem das erzeugte X.509-Zertifikat (hexstring [X.690] DER-codiert) und der zugehörige private Schlüssel (hexstring [RFC5915] DER-codiert) übermittelt werden.

Beispiel 4.1.

4.4.9.5 Technische Anwendungsfälle

Das Kommunikationsszenario verwendet folgende technische Anwendungsfälle deren Detailanforderungen in [DS]) beschrieben sind:

- Aktives Öffnen einer TCP-Verbindung (Initiieren)
- Öffnen einer TLS-Session als Client
- Erzeugen eines HTTP-Requests
- Verarbeiten einer HTTP-Response
- Schließen der TCP/TLS-Verbindung nach Empfang eines CloseNotify Alerts
- Schließen der TCP/TLS-Verbindung, initiiert durch den CLS-Kommunikationsadapter

In der Default-Konfiguration **MUSS** der CLS-Kommunikationsadapter den TCP-Port 443 für den HTTP-Service zum SMGW verwenden. [REQ.HKS.WS1.CLI.50]

Der CLS-Kommunikationsadapter **MUSS** im TLS-Handshake die Extension "Application Layer Protocol Negotiation" mit alpn = "http/1.1" senden. [REQ.HKS.WS1.CLI.60]

5 Anforderungen an die IT-Sicherheit

5.1 BSZ zum Erfüllen der Sicherheitsziele an die Einsatzumgebung von SMGW

CLS-Komponenten sind bei Vorhandensein von nicht durch das SMGW abgesicherten Verbindungen in weitere Netzwerke nicht vollumfänglich durch die Sicherheitsleistung des nach Common Criteria zertifizierten SMGW geschützt. Dies wird bereits im Schutzprofil des SMGW [PP-0073] adressiert, in dem das Sicherheitsziel für die Einsatzumgebung (Security Objective for the Operational Environment) **OE.Network** genau diesen Sachverhalt abbildet. Dort wird gefordert:

> *It shall be ensured that [...] if devices in the HAN have a separate connection to parties in the WAN (beside the Gateway) this connection is appropriately protected.* [Es muss sichergestellt werden, dass, [...] wenn Geräte im HAN eine separate Verbindung zu Entitäten im WAN (abgesehen vom Gateway) haben, diese Verbindung angemessen geschützt ist.]

Die in dieser TR betrachteten CLS-Kommunikationsadapter setzen die kommunikative Anbindung an die HAN-Schnittstelle des SMGW und damit die Einbindung von CLS-Komponenten in das HAN des SMGW um. CLS-Komponenten, für die eine Zertifizierung nach dieser TR möglich ist, können weitere, nicht durch das SMGW abgesicherte Verbindungen in weitere Netzwerke aufweisen. Eine IT-Sicherheitszertifizierung nach BSZ ist nur dann notwendig, wenn dies für die CLS-Komponente nach ▸Abschnitt 2.9 festgestellt wurde (siehe ▸REQ.GEN.Schnittstellen.10). Die BSZ betrachtet die gesamte CLS-Komponente, die den CLS-Kommunikationsadapter realisiert. [1] Daher steht in diesem Kapitel und für die Formulierung der IT-Sicherheitsanforderungen die CLS-Komponente im Fokus.

Es ist zu beachten, dass **OE.Network** stets in der Einsatzumgebung des SMGW zu erfüllen ist; unabhängig davon, ob eine CLS-Komponente oder allgemeiner eine Komponente im HAN des SMGW nach dieser TR zertifiziert wird.

Das Schema der BSZ ist ein Produktzertifizierungsverfahren mit risikobasiertem Ansatz und bestätigt Sicherheitsaussagen über ein IT-Produkt in Form eines Zertifikats. Durch belastbare Zeit- und Kostenplanung können Aufwände für Hersteller gering gehalten und gleichzeitig ein hohes Vertrauensniveau in die Sicherheitsleistung des Produkts erzeugt werden. Die BSZ legt den Fokus der Evaluation auf Penetrationstests. Darüber hinaus werden Herstellerdokumentation und implementierte kryptographische Mechanismen bewertet. Die Kommunikationsschleifen zwischen Hersteller, Prüfstelle und Zertifizierungsstelle werden auf ein absolut notwendiges Maß reduziert.

Für die TR wird daher der neue BSZ-Geltungsbereich "Komponenten im HAN des SMGW" etabliert, in dem Anforderungen an das Verfahren der Prüfung von CLS-Komponenten gestellt werden. Darunter fallen unter anderem Vorgaben an die Prüfstellen, sowie die in dieser TR aufgestellten Mindestanforderungen bezüglich der IT-Sicherheit an den Evaluierungsgegenstand (englisch Target of Evaluation), aber auch Anforderungen an die Erstellung eines Security Target (ST). In einem ST bilden Hersteller die Sicherheitsvorgaben an den Evaluierungsgegenstand und insbesondere das Sicherheitsproblem ab. Dieses Sicherheitsproblem wird in den Dokumenten des BSZ-Geltungsbereichs "Komponenten im HAN des SMGW" vorgegeben, um die besonderen Gegebenheiten des SMGW und seiner Umgebung zu berücksichtigen. Es wird in ▸Abschnitt 5.2 abgebildet. In ▸Abschnitt 5.3 sind die Sicherheitsanforderungen an die CLS-Komponente beschrieben. Die Prüfung dieser Sicherheitsanforderungen erfolgt allerdings nicht im Rahmen der TR-Konformitätsprüfung, sondern im Rahmen des BSZ-Zertifizierungsverfahrens.

In ▸Abschnitt 5.4 sind die Anforderungen an CLS-Komponenten im Zusammenhang mit der BSZ formuliert, die im Rahmen dieser TR geprüft werden, wenn dies für die CLS-Komponente nach ▸Abschnitt 2.9 festgestellt

[1] Die Sicherheitsaussage einer BSZ-Zertifizierung bezieht sich immer auf die untersuchte und geprüfte CLS-Komponente. Es ist möglich, diese zertifizierte CLS-Komponente beispielsweise innerhalb einer nachgelagerten Komponente als Ganzes zu integrieren. Erfolgt dies, muss die nachgelagerte Komponente nicht selbst nach TR-5 zertifiziert werden. Dabei überträgt sich die Sicherheitsaussage für die CLS-Komponente nicht auf die nachgelagerte Komponente.

wurde (siehe ▸REQ.GEN.Schnittstellen.10) . Die Prüfung aller weiteren Anforderungen in diesem Kapitel erfolgt nicht im Rahmen der TR-Konformitätsprüfung, sondern im Rahmen des BSZ-Zertifizierungsverfahrens.

5.2 Sicherheitsproblem und Einsatzumgebung

5.2.1 Einleitung

Die Dokumente für den Geltungsbereich "Komponenten im HAN des SMGW" beinhalten unter anderem Anforderungen an das ST.

Im ST werden die Sicherheitsfunktionen, die zulässige Einsatzumgebung und das Sicherheitsproblem für den Evaluierungsgegenstand beschrieben. Das Sicherheitsproblem ist Teil des Abschnitts "Sicherheitsumfang" (security perimeter). In diesem werden für einen Evaluierungsgegenstand die Akteure (User), Annahmen (Assumptions), schützenswerten Güter (Assets) mit jeweiligem Schutzbedarf sowie die betrachteten Angreifer (Attacker) und Bedrohungen (Threats) definiert.

Für den BSZ-Geltungsbereich "Komponenten im HAN des SMGW" werden dieses Sicherheitsproblem und ebenso Anforderungen an die Einsatzumgebung durch ein ST-Template vorgegeben, hierbei definiert der Hersteller das Sicherheitsproblem nicht selbst. Dieses Sicherheitsproblem, die Anforderungen an die Einsatzumgebung, sowie die weiteren Vorgaben an das ST sind in den Dokumenten des BSZ-Geltungsbereichs "Komponenten im HAN des SMGW" definiert. In den folgenden Abschnitten werden sowohl die Akteure, Annahmen, schützenswerten Güter, Angreifer und Bedrohungen für das Sicherheitsproblem als auch Anforderungen an die Einsatzumgebung vorgegeben.[2] Für weitere Informationen und die Implementierung dieser Anforderungen in ein herstellereigenes ST wird auf die Dokumente des BSZ-Geltungsbereichs "Komponenten im HAN des SMGW" verwiesen.

5.2.2 Akteure

Das Sicherheitsproblem für CLS-Komponenten betrachtet mindestens diejenigen Akteure (User) aus ▸Abschnitt 2.6, die mit der CLS-Komponente interagieren.

Es umfasst darüber hinaus die in ▸ICS.GEN.Akteure.10 und ▸ICS.FA.FwInstallation.10 deklarierten Akteure.

Zudem ist in der BSZ die technische Rolle des Administrators eines Evaluierungsgegenstands vorgesehen. Diese technische Rolle ist notwendig, um Konfigurationen und Managementtätigkeiten durchzuführen, damit der Evaluierungsgegenstand in seiner sicheren (d.h. zertifizierten) Konfiguration ist und bleibt. Wie und von wem diese technische Rolle umzusetzen ist, wird im Geltungsbereich "Komponenten im HAN des SMGW" nicht vorgegeben.

5.2.3 Annahmen

Das Sicherheitsproblem für CLS-Komponenten trifft die folgenden Annahmen:

Assumption.TrustedAdmin: Der Administrator der CLS-Komponente ist vertrauenswürdig und angemessen geschult.

Assumption.CertifiedSMGW: Das SMGW, in dessen HAN sich die CLS-Komponente befindet, ist nach [PP-0073] und [TR-03109-1] zertifiziert und wird im zertifizierten Zustand betrieben.

Assumption.TrustedDataHandling: Es wird angenommen, das autorisierte Benutzer, die nach entsprechender Authentisierung und Autorisierung auf Daten, die sich auf der CLS-Komponente befinden, zugreifen oder diese erhalten, vertrauenswürdig im Kontext dieser Daten sind.

Assumption.CertifiedUpdate: Die Firmware-Updates für die CLS-Komponente, die von einem autorisierten Nutzer bereitgestellt werden können, wurden vor Auslieferung gemäß BSZ, Geltungsbereich "Komponenten im HAN des SMGW", zertifiziert, um sicherzustellen, dass das Update korrekt implementiert wurde. Der Nutzer, der zum Aufbringen des Updates autorisiert ist, ist vertrauenswürdig und stellt sicher, dass keine Schadsoftware über das Firmware-Update eingebracht wird.

[2] Um die direkte Verwendung des Sicherheitsproblems im BSZ-Security-Target (ST) zu vereinfachen, wird die englische Sprache für die notwendigen eindeutigen Bezeichner (ID) verwendet.

Assumption.PhysicalProtection: Es wird angenommen, dass die CLS-Komponente in einer nicht-öffentlichen Umgebung betrieben wird. Diese Umgebung gewährt einen grundlegenden physischen Schutz. Insbesondere bedeutet das:

- Der lokale physische Angreifer hat nur begrenzten physischen Zugriff auf die CLS-Komponente: der Zeitraum für einen Angriff ist auf insgesamt 10 Minuten beschränkt. Außerdem kann der Angreifer die CLS-Komponente nicht von ihrem angebrachten Ort entfernen.
- Es kann angenommen werden, dass eine regelmäßige Sichtinspektion der CLS-Komponente stattfindet. Dies bedeutet, dass Bohr-, Schneid- und Fräs-Angriffe auf ständig sichtbaren Oberflächen vernachlässigt werden können.

Assumption.Network: Es wird angenommen, dass für Geräte, die an die CLS-Komponente angeschlossen sind und die eine Verbindung in weitere Netzwerke aufweisen (abgesehen von der Verbindung über den, vom CLS-Kommunikationsadapter der CLS-Komponente bereitgestellten, TLS-Proxy-Kanal des SMGW), diese Verbindung angemessen abgesichert ist.

5.2.4 Angreifer

Im Sicherheitsproblem für CLS-Komponenten wird zwischen vier möglichen Angreifern entsprechend ihrer Angriffspfade unterschieden. Die Angriffspfade unterscheiden sich danach, welche Schnittstelle der CLS-Komponente für den Angriff verwendet wird und wo der Angreifer verortet ist. Dafür ist insbesondere die Art der Schnittstelle nach ▸Tabelle 2.1 ausschlaggebend.

- **Attacker.LocalPhys**: Ein Angreifer mit physischem Zugriff auf die CLS-Komponente. Primäres Ziel des Angreifers ist die Umgehung des Gehäuses, um auf nicht dokumentierte Schnittstellen zuzugreifen (z.B. zur Freilegung eines Debug-Ports oder von Chip-Pins.) Der Angreifer verwendet ausschließlich eine Auswahl von Werkzeugen geringer Größe[3], die geringe Expertise benötigen und einfach zu beschaffen sind[4]. Folgende Werkzeuge werden von dieser Definition unter anderem erfasst (nicht notwendigerweise abschließend):
  - Schraubendreher
  - Heißluftpistolen, Kältespray
  - Gewöhnliche Lösungsmittel wie etwa Isopropylalkohol oder Azeton.
  - Lötkolben, Kabel und Klemmen bzw. Stecker
- **Attacker.LocalIT**: Ein Angreifer greift über eine lokale IT-Schnittstelle auf die CLS-Komponente zu. Ein Beispiel für solch eine lokale IT-Schnittstelle ist eine lokale Ethernet-Schnittstelle.
- **Attacker.Radio**: Ein Angreifer in Funkreichweite nutzt funkbasierte Schnittstellen der CLS-Komponente aus, um auf sie zuzugreifen. Darunter fällt zum Beispiel eine wM-Bus-Schnittstelle.
- **Attacker.Remote**: Ein Angreifer in einem Weitverkehrsnetz greift über die Fernzugriffsschnittstelle der CLS-Komponente oder über eine lokale IT-Schnittstelle, die über ein Weitverkehrsnetz erreichbar ist, auf diese zu. Darunter fällt zum Beispiel eine LTE-Verbindung.

Die Angriffspfade sind in ihrer Kritikalität aufsteigend gelistet: während der Angreifer in einem lokalen Netzwerk nur eine CLS-Komponente bedroht, sind für den Angreifer in Funkreichweite alle CLS-Komponenten innerhalb dieser Reichweite angreifbar. Der Angreifer im Weitverkehrsnetz schließlich kann potenziell alle CLS-Komponenten mit Fernzugriffsschnittstelle gleichermaßen angreifen.

5.2.5 Bedrohungen

Die Bedrohungen sind unabhängig von der Art des Angriffspfads. Folgende Bedrohungen sind für CLS-Komponenten mindestens relevant:

- **Threat.AccessHAN**: Über die CLS-Komponente kann unberechtigterweise auf das HAN des SMGW zugegriffen werden, wodurch der Schutz der weiteren Komponenten im HAN des SMGW nicht mehr ausreichend gewährleistet werden kann.

[3] D.h. Werkzeuge, die zusammen in einen regulären Rucksack passen.

[4] Also für Privatpersonen im Handel erhältlich sind.

- **Threat.CompromiseAssets**: Ein Angreifer[5] modifiziert, eliminiert oder liest schützenswerte Güter (*Assets*), die auf der CLS-Komponente enthalten sind, entgegen ihrem Schutzziel aus.

Sowohl die Bedrohung Threat.AccessHAN als auch Threat.CompromiseAssets beinhalten unter anderem den Angriffsweg über an die CLS-Komponente angeschlossene nachgelagerte Komponenten.

5.2.6 Assets

Die Assets, die auf einer CLS-Komponente vorliegen können, sind in ▸Tabelle 5.1 aufgelistet, ergänzt durch die entsprechenden Schutzbedarfe.

ID	Asset	Beschreibung	Schutzbedarf
Asset.PII	Personenbezogene Daten	Personenbezogene Daten gemäß DSGVO, d.h. alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dies umfasst auch Informationen, die in der CLS-Komponente persistiert werden, die in der Liegenschaft generiert werden und mit dieser assoziiert werden, also von der Verortung der CLS-Komponente abhängen.	Vertraulichkeit, Integrität[6]
Asset.Certs	Zertifikatsmaterial	Kryptographisches Material, das von der CLS-Komponente für die Prüfung von digitalen Signaturen verwendet wird, wie etwa öffentliche Schlüssel und Zertifikate.	Integrität, Authentizität
Asset.Keys	Kryptographisches Schlüsselmaterial	Privates Schlüsselmaterial, das von der CLS-Komponente für kryptographische Operationen verwendet wird.	Vertraulichkeit, Integrität, Authentizität
Asset.Config	Konfigurationsdaten	Daten, die Konfigurationsinformationen für den Betrieb der CLS-Komponente enthalten, etwa Zugriffsberechtigungen für Akteure oder Informationen zur Kommunikation mit weiteren Entitäten. Zu Letzterem gehören u.a. ProxyIds, Adressen für SMGW oder nachgelagerte steuerbare Einrichtungen.	Integrität, Authentizität
Asset.AuthData	Authentisierungsdaten (Passwort-Hashes, Cookies, User IDs)	Material, das von der CLS-Komponente für Operationen zur Authentifizierung von Akteuren verwendet wird.	Vertraulichkeit, Integrität, Authentizität
Asset.FWUpdate	Firmware-Update	Die binäre Repräsentation von zur Aktualisierung der Firmware geeigneten Daten zur Übertragung und Speicherung.	Integrität, Authentizität
Asset.TlsProxyData	TLS-Proxy-Daten	Daten, die die CLS-Komponente über den TLS-Proxy-Kanal erhält oder versendet. Ist eine Obermenge zu anderen gelisteten Assets.	(Vertraulichkeit,) Integrität, Authentizität
Asset.Time	Systemzeit	Zeit der CLS-Komponente.	Integrität, Authentizität
Asset.SysLog	Systemlog	Log, das Einträge über sicherheits- und systemrelevante Ereignisse enthält.	Vertraulichkeit, Integrität

Tabelle 5.1 Assets und Schutzziele

Das Sicherheitsproblem für die CLS-Komponente kann noch zusätzliche Assets und Schutzbedarfe berücksichtigen, sofern diese vom Hersteller im ST ergänzt werden. Beispiele sind in Tabelle ▸Tabelle 5.2 aufgeführt.

[5] Dazu zählen auch authentifizierte Akteure, die keinen Zugriff auf die innerhalb eines Assets hinterlegten Informationen haben dürfen.

[6] Falls zutreffend, können weitere Schutzbedarfe im Rahmen der BSZ im Security Target betrachtet werden, z.B. solche, die sich aus einer Datenschutzfolgeabschätzung gemäß DSGVO ergeben.

ID	Asset	Beschreibung	Schutzbedarf
Asset.ControlData	Steuerungsdaten	Daten, die zur Steuerung von steuerbaren Einrichtungen verwendet werden.	Integrität, Authentizität
Asset.SensorData	Sensordaten	Daten, die zum Beispiel von Sensoren nachgelagerter Einrichtungen erfasst und bereitgestellt werden.	Vertraulichkeit, Integrität, Authentizität

Tabelle 5.2 Beispiele für zusätzliche Assets und Schutzziele

5.2.7 Einsatzumgebung

Es sind zusätzlich Vorgaben an die Einsatzumgebung von CLS-Komponenten nötig. Dabei wird nicht nur die CLS-Komponente selbst, sondern auch deren Interaktion mit weiteren Geräten berücksichtigt. Daraus folgt, dass mit der BSZ Auflagen an den Betrieb der CLS-Komponente verbunden sein können, um die Vorgaben an die Einsatzumgebung zu berücksichtigen. Eine anderweitige Verwendung entspricht nicht der zertifizierten Konfiguration.

5.3 Sicherheitsfunktionalität

Die Funktionalität, die die CLS-Komponente implementiert, um den Bedrohungen auf die Assets, die auf der CLS-Komponente vorhanden sind, zu begegnen, wird Sicherheitsfunktionalität genannt. Die CLS-Komponente muss die folgenden Mindestanforderungen an die Sicherheitsfunktionalität umsetzen, wenn dies für die CLS-Komponente nach ▸Abschnitt 2.9 festgestellt wurde (siehe ▸REQ.GEN.Schnittstellen.10). Die Prüfung der Implementierung der Sicherheitsfunktionen wird innerhalb des Zertifizierungsverfahrens der BSZ durchgeführt.

Authentisierung und Autorisierung: Es werden Mindestanforderungen an die Identifikation und Authentisierung von Nutzern gestellt sowie unter anderem ein Rollenmanagement gefordert.

1. Die CLS-Komponente muss[7] den Nutzer[8] an der jeweiligen Schnittstelle identifizieren und authentisieren, bevor dieser auf die Services (der CLS-Komponente) zugreifen kann. Hinweis: Eine anonyme Nutzung kann möglich sein, wenn eine Kompromittierung der CLS-Komponente nicht möglich ist und keine kritische Konfiguration geändert werden kann.
2. Die CLS-Komponente muss sich dem Nutzer gegenüber eindeutig identifizieren und sich authentisieren können.
3. Die CLS-Komponente soll die Administration aller vorhandenen Nutzerkonten ermöglichen.
4. Die CLS-Komponente muss die Änderung von Authentisierungsdaten, z.B. Passwörter und Nutzernamen, ermöglichen und muss diese Authentisierungsdaten vor unautorisiertem Zugriff schützen.
5. Die CLS-Komponente muss ein Rollen-Management für den Zugriff auf Dateien, Daten und Services bieten. Zugriffsrechte müssen restriktiv vergeben werden.
6. Die CLS-Komponente muss Administratoren mit User-Management-Funktionalität ausstatten, die mindestens das Zuweisen, Bearbeiten und Entziehen von Zugriffsrechten umfasst.
7. Die CLS-Komponente darf keine hart-kodierten kryptographischen Geheimnisse (z.B. Passwörter, kryptographische Schlüssel oder andere Berechtigungsnachweise) enthalten, die von verschiedenen Produkten geteilt werden.
8. Die CLS-Komponente muss hinreichende Entropie und Sicherheit von Passwörtern bei deren Erstellung und Änderung erzwingen. Das Verhalten muss der in den Handbüchern beschriebenen Passwort-Richtlinie entsprechen.
9. Die CLS-Komponente darf als Reaktion auf Authentisierung keine sicherheitsrelevanten Informationen preisgeben oder Rückschlüsse auf sicherheitsrelevante Informationen ermöglichen.

[7] In Kapitel 5 werden die Schlüsselwörter aus ▸Abschnitt 1.9 klein geschrieben, da diese nicht im Rahmen der TR-Konformitätsprüfung, sondern innerhalb des BSZ-Verfahrens geprüft werden.

[8] Personen, Organisationseinheiten oder automatisierte Prozesse (Dienste), die oder auf die die CLS-Komponente zugreift.

10. Die CLS-Komponente muss Authentisierungsversuche limitieren, um Brute-Force-Angriffen vorzubeugen.
11. Die CLS-Komponente muss nach einer bestimmten Zeit der Inaktivität und nach einer festgelegten Zeitspanne (maximal 48 Stunden) eine erneute Authentisierung verlangen.
12. Die CLS-Komponente muss für eine Benutzeroberfläche[9] nach einer bestimmten Zeit der Inaktivität (maximal 10 Minuten) eine erneute Authentisierung verlangen.

Logging: Es werden Mindestanforderungen an die zu protokollierenden Informationen und Daten sowie an den Zugang und die Speicherung des Logs gestellt.

1. Die CLS-Komponente muss mindestens die folgenden Events protokollieren:
   - Fehlerhafte Authentisierung
   - Initialisierung und Erfolg/Misserfolg des Firmware-Updates
   - Initialisierung und Wiederherstellen eines Backups
   - Änderungen an der Konfiguration
2. Für die obengenannten Events muss die CLS-Komponente die folgenden Informationen speichern:
   - Zeitstempel
   - Event ID
   - Event-Typ
   - Ursprung des Events (ID des Nutzers oder des Software-Prozesses von dem das Event stammt)
   - Ergebnis des Ereignisses, das das Event ausgelöst hat
3. Die CLS-Komponente muss hinreichend viel lokalen Speicherplatz für die Protokollierung von Events zur Verfügung stellen.
4. Die CLS-Komponente muss ihre Sicherheitsfunktionalität (möglicherweise mit Ausnahme der Protokollierung) aufrecht erhalten, falls nicht genügend Speicherplatz zur Verfügung steht.
5. Die CLS-Komponente muss den Zugang zu Protokollierungsdaten auf autorisierte Nutzer beschränken, die gemäß der Beschreibung der entsprechenden Assets im ST hinsichtlich dieser Informationen zugriffsberechtigt sind.

Services: Diese Mindestanforderungen behandeln unter anderem zulässige Status der CLS-Komponente, Backups, Firmware-Updates sowie den Umgang mit Fehlermeldungen.

1. Die CLS-Komponente muss robust auf falsche oder fehlerhafte Daten ihrer Services reagieren.
2. Die CLS-Komponente darf zu keinem Zeitpunkt in einen undefinierten Zustand gelangen.
3. Die CLS-Komponente muss die Integrität, Authentizität und Vertraulichkeit übermittelter Daten entsprechend dem Schutzbedarf der jeweiligen Assets schützen.
4. Die CLS-Komponente muss Eingaben und Ausgaben validieren, bevor sie verarbeitet werden, um fehlerhafte Verarbeitung zu vermeiden.
5. Die CLS-Komponente muss Fehler adäquat behandeln.
6. Die CLS-Komponente darf in Fehlermeldungen keine kritischen Informationen[10] preisgeben.
7. Die CLS-Komponente muss eine Funktionalität zum Zurücksetzen auf Standardkonfiguration mit der aktuellsten Firmware bereitstellen. Zu diesem Zweck muss eine Funktionalität vorhanden sein, die alle personenbezogenen Daten sicher und zuverlässig löscht.
8. Die CLS-Komponente muss Funktionalität für Backups und die Wiederherstellung der aktuellen Konfiguration bereitstellen.

[9] Benutzeroberfläche ist die Schnittstelle zwischen CLS-Komponente und Personen.

[10] Kritische Informationen sind Informationen, die für potenzielle Angreifer relevanten Informationen enthalten. Beispielsweise dürfen die Protokolldateien keine Authentifizierungsdaten enthalten.

9. In der Standardkonfiguration sollten nur Services in der CLS-Komponente aktiviert sein, die notwendig sind, um die Basisfunktionalität auszuführen. Es muss eine Möglichkeit für Nutzer bestehen, nicht notwendige Services zu deaktivieren.
10. Nur Services und Software, die benötigt sind, um die Funktionalität der CLS-Komponente bereitzustellen, dürfen auf der CLS-Komponente vorhanden sein. Entwicklungsinformationen müssen entfernt werden.
11. Die CLS-Komponente muss die Möglichkeit für Firmware-Updates bereitstellen.
12. Die CLS-Komponente muss die Möglichkeit, ein Firmware-Update zu initiieren, auf Administratoren und die CLS-Komponente selbst beschränken.
13. Die CLS-Komponente muss vor der Installation eines Firmware-Updates die Authentizität und Integrität der Firmware-Update-Dateien bestätigen.
14. Die CLS-Komponente muss bestätigen, dass die Version des Firmware-Updates, das installiert werden soll, neuer ist als die aktuell installierte Version.
15. Der Zugang zu drahtlosen Netzwerken muss abgesichert sein.

Grundlegender physischer Schutz: Es werden Mindestanforderungen an den physischen Schutz gestellt, insbesondere müssen Maßnahmen derart ergriffen werden, dass physische Manipulation von außen erkannt wird.

1. Die CLS-Komponente muss Maßnahmen implementieren, um physische Angriffe zu erschweren, d.h. das Gehäuse der CLS-Komponente muss so kreiert sein, dass es innere Bauteile schützt, das Umgehen des Gehäuseschutzes vermieden wird und dass es nicht einfach geöffnet werden kann, ohne dass dies erkannt wird. Insbesondere muss die CLS-Komponente eine Manipulationserkennung bieten, d.h. nach einem Manipulationsversuch müssen (physische oder digitale) Beweise zurückbleiben.
   - Das Gehäuse der CLS-Komponente muss jegliche Schnittstellen, die im ST nicht als zugängliche Schnittstellen erwähnt sind, vor direktem physischen Zugang schützen, d.h., das Gehäuse darf keine kritischen Leiterbahnen oder essenziellen Bauteile exponieren.
   - Wenn das Gehäuse der CLS-Komponente sichtbare Schrauben aufweist, müssen Sicherheitsschrauben verwendet werden.
   - Deckel, Klappen und aufsetzbare Teile des Gehäuses der CLS-Komponente müssen so an dem Gehäuse befestigt werden, dass eine Entfernung die Erkennung dieser Manipulation ermöglicht. Beispielsweise können diese Teile mittels Siegeln mit dem Gehäuse der CLS-Komponente verbunden werden.

Kryptographie: Zusätzlich zu den Mindestanforderungen, die in [AIS B2] bereits formuliert sind, werden ergänzende oder sie verschärfende Anforderungen an die kryptographischen Operationen gestellt.

1. Die CLS-Komponente muss kryptographische Operationen gemäß den Anforderungen in [AIS B2] durchführen. Zusätzlich muss die CLS-Komponente die folgenden, ergänzenden Anforderungen umsetzen, die die Anforderungen in [AIS B2] verschärfen oder weitere Details ergänzen.
2. Die CLS-Komponente darf nicht Algorithmen des SOG-IS Katalogs [SOGIS-Crypto] verwenden, die als "legacy" markiert sind.
3. Die CLS-Komponente soll nur kryptographische Mechanismen verwenden, die den Empfehlungen der [TR-02102-1] folgen.
4. Für die Kommunikation mit nachgelagerten Komponenten soll die CLS-Komponente TLS gemäß [TR-02102-2] verwenden.
5. Wenn die CLS-Komponente die kryptographischen Protokolle TLS, IPSec oder SSH verwendet, muss die CLS-Komponente diese Protokolle gemäß [TR-02102-2], [TR-02102-3] bzw. [TR-02102-4] implementieren. Die Empfehlungen innerhalb dieser Dokumente müssen befolgt werden.
6. Für die Kommunikation mit dem SMGW muss die CLS-Komponente ausschließlich die kryptographischen Mechanismen gemäß [TR-03109-3] verwenden.
7. Wenn die CLS-Komponente ein Protokoll oder einen Standard verwendet, für den ein Sicherheitsprofil oder eine Sicherheitserweiterung existiert, soll diese Sicherheitserweiterung verwendet werden.

Es ist zu beachten, dass je nach CLS-Komponente weitere Sicherheitsfunktionalität zusätzlich zur Erfüllung dieser Mindestanforderungen notwendig ist, um dem zugehörigen spezifischen Sicherheitsproblem, das der Hersteller im ST beschreibt, zu begegnen.

Darüber hinaus müssen für eine Prüfung im BSZ-Geltungsbereich "Komponenten im HAN des SMGW" dort aufgeführte Dokumente, unter anderem das ST und Handbücher, erstellt werden. Anforderungen an das ST werden im ST-Template formuliert, zudem gelten die Anforderungen in [AIS B1]. Anforderungen an die Handbücher umfassen unter anderem die getroffenen Annahmen und die zulässige Einsatzumgebung, Hinweise zur sicheren Nutzung, den Umgang mit Fehlermeldungen sowie Möglichkeiten zur Identifikation der CLS-Komponente und ihrer Version. Die Anforderungen in [AIS B3] gelten zusätzlich.

5.4 Sicherheitszertifizierung

Gemäß ▸REQ.GEN.Schnittstellen.10 ist für eine CLS-Komponente, die Fernzugriffsschnittstellen oder lokale IT-Schnittstellen aufweist, eine Zertifizierung nach BSZ im Geltungsbereich "Komponenten im HAN des SMGW" notwendig. Das bedeutet, dass die IT-Sicherheitsprüfung der CLS-Komponente an sich sowie die Prüfung der Dokumentation und die Prüfung des ST im Rahmen der BSZ erfolgen. Insbesondere geschieht die Prüfung der Konformität des ST des Herstellers zu den Anforderungen an das ST-Template innerhalb der BSZ und nicht im Rahmen der TR-Zertifizierung. In der BSZ wird also u.a. geprüft, ob das ST des Herstellers die in ▸Abschnitt 5.2 abgebildeten Inhalte enthält. Im Rahmen der TR-Konformitätsprüfung wird zusätzlich eine Konsistenzprüfung zwischen der Produktbeschreibung im ST und den Angaben der ICS durchgeführt.

Das der Zertifizierung zugrundeliegende BSZ-Security Target (ST) **MUSS** eine Produktbeschreibung ("Product Description") enthalten, die zu den Angaben der ICS in ▸Abschnitt 2.9 konsistent ist. [REQ.ITS.BSZ.20]

6 Weitere Anforderungen

6.1 Anforderungen an die Handbücher

Die Handbücher der CLS-Komponente **MÜSSEN** für die Akteure, an die die Handbücher adressiert sind, verständlich sein. [REQ.GEN.Dokumentation.30]

Die Handbücher der CLS-Komponente **MÜSSEN** zu den Angaben des Herstellers in den ICS konsistent sein. [REQ.GEN.Dokumentation.40]

6.2 Identifikation und Aufschriften der CLS-Komponenten

Damit eine CLS-Komponente sowohl für informationstechnische Systeme, für Personen bei der Installation und auch im Wirkbetrieb identifizierbar ist, werden Anforderungen an die Einheitlichkeit und Interoperabilität der Identifikation gestellt.

Insbesondere für die initiale kommunikative Anbindung ist es für den Nutzer der CLS-Komponente wichtig, dass die kryptographische Identität (das Schlüsselpaar) und die Identifikation der CLS-Komponente als Besitzer des Schlüsselpaares richtig miteinander verknüpft sind.

Das Gehäuse der CLS-Komponente **MUSS** mit einer herstellerübergreifend eindeutigen Identifikation ablesbar beschriftet sein. [REQ.GEN.Identifikation.10]

Die herstellerübergreifend eindeutige Identifikation der CLS-Komponente **MUSS** in der kanonisierten Repräsentation (ohne Leerzeichen, 14-stellig) gemäß [DIN43849] gebildet werden. [REQ.GEN.Identifikation.20]

Die SubjectCN des CLS-Zertifikates des CLS-Kommunikationsadapters **MUSS** die herstellerübergreifend eindeutige Identifikation der CLS-Komponente enthalten. [REQ.GEN.Identifikation.30]

Auf dem Gehäuse der CLS-Komponente **MUSS** die Typ-Bezeichnung der CLS-Komponente ablesbar sein, die der in der CLS-Dokumentation der Komponente entspricht. [REQ.GEN.Identifikation.40]

Auf dem Gehäuse der CLS-Komponente **MUSS** im Sichtbereich die Zertifizierungskennzeichnung gemäß BSI-Zeichenordnung in einer Fläche mit den Abmessungen 1cm x 2cm angebracht werden. [REQ.GEN.Identifikation.50]

Glossar

Acceptor	Empfänger oder Empfängerin einer Nachricht.
aktiver Externer Marktteilnehmer	Technische Rolle in der PKI des iMSys, siehe [SM-PKI-CP], die berechtigt ist, über den TLS-Proxy-Kanal des SMGW Komponenten im HAN des SMGW anzusprechen. Ist gleichzeitig für seine Zwecke datenumgangsberechtigtes Unternehmen.
Asset	Auch: Schützenswertes Gut. Datum oder Material, das vor unberechtigtem Zugriff, Entfernen oder Manipulation zu schützen ist.
CLS-Kommunikationsadapter	Logische Einheit, die zur Nutzung der vom SMGW bereitgestellten *TLS-Proxy-Funktion* vorgesehen ist und die den TLS-Endpunkt dieses TLS-Proxy-Kanals im *HAN des SMGW* darstellt. Ist Teil einer (physischen) *CLS-Komponente*.
CLS-Komponente	Physische *Komponente im HAN des SMGW*, die einen *CLS-Kommunikationsadapter* realisiert. Wird mithilfe des CLS-Kommunikationsadapters kommunikativ an die HAN-Schnittstelle des SMGW angebunden.
Ereignis	(engl. event) Auftreten eines nachweisbaren oder feststellbaren Geschehens im Programmablauf einer Komponente. Ereignisse können beispielsweise Fehler oder Zustandsänderungen sein.
Fachlicher Anwendungsfall	Beschreibt genau eine Aufgabenstellung, die aufgrund interner oder externer *Ereignisse* von einer Komponente abgearbeitet wird.
Firmware	Auf der Hardware der Komponente ausgeführte Anweisungen zum Betrieb und der Informationsverarbeitung.
Firmware-Update	Die binäre Repräsentation von zur Aktualisierung der *Firmware* geeigneten Daten zur Übertragung und Speicherung.
GW_HAN_TLS_CRT	Das TLS-Authentifizierungszertifikat des SMGW an der HAN-Schnittstelle gemäß HAN-Zertifikatsprofil ([DS]) basierend auf [RFC5280] Kapitel 4.
HAN des SMGW	HAN-Netzwerk gemäß [PP-0073]. Umfasst das gesamte, an der HAN-Schnittstelle des SMGW aufgespannte Netzwerk, aus dem das SMGW kommunikativ ohne Routing[1] erreicht werden kann.
ICMPv4	In [RFC0792] spezifiziertes (Fehler-)Signalisierungsprotokoll, eingeschränkt durch [RFC6918].
ICMPv6	In [RFC4443] spezifiziertes (Fehler-)Signalisierungsprotokoll.
IF_GW_CLS	Logische Schnittstelle des SMGW, die CLS-Komponenten die Kommunikation mit Kommunikationspartnern im WAN des SMGW über den *TLS-Proxy-Kanal* des SMGW ermöglicht, siehe [PP-0073] und [TR-03109-1].
IPv4	In [RFC0791], [RFC1122] und [RFC3927] spezifiziertes Netzwerkprotokoll.
IPv6	In [RFC8200] und [RFC8504] spezifiziertes Netzwerkprotokoll.
IT-Schnittstelle	Logische oder physische informationstechnische Schnittstelle, durch die ein Zugriff auf den CLS-Kommunikationsadapter und seine Funktionen möglich ist.
kanonisierte Form	Zur Verarbeitung und zum Vergleich normalisierte Darstellung mit fester Länge, ohne Leerzeichen.

[1] (Paket) Forwarding wird hierbei als Teilmenge des Routings gesehen.

Kommunikationsadapter	Logische Einheit, die die einheitliche und sichere kommunikative Anbindung an das SMGW unterstützt. Ist in einer physischen Komponente realisiert.
Kommunikationspartner im WAN	Externe Entität im WAN des SMGW, mit der die Komponente im HAN des SMGW über einen *TLS-Proxy-Kanal* kommunizieren kann.
Kommunikationsprofil	Ein Oberbegriff für Profile zur Festlegung von Parametern für die Kommunikation. Ein Kommunikationsprofil kann durch eine oder mehrere Datenstrukturen realisiert werden.
Kommunikationsszenario	Beschreibt die Komposition des Protokollstapels und die Datenflussrichtungen an einer Schnittstelle zwischen einer Komponente im HAN des SMGW und einem weiteren Akteur.
Komponente im HAN des SMGW	Physisches Gerät, das direkt mit der HAN-Schnittstelle des SMGW auf IP-Ebene interagiert. Siehe auch *HAN des SMGW*.
lokaler Nutzer/lokale Nutzerin	Lokaler Akteur oder Akteurin im HAN des SMGW, interagiert dort mit einer Komponente. Kann die Komponente zum Beispiel zur lokalen Interaktion mit dem SMGW nutzen.
nachgelagerte Komponente	Physisches Gerät (z.B. Wechselrichter), das mit einer *CLS-Komponente* (z.B. Steuerungseinrichtung) interagieren kann, sich aber selbst nicht im HAN des SMGW befindet.
Originator	Erzeuger/Erzeugerin und Absender/Absenderin einer Nachricht.
ProxyId	Identifiziert im SMGW das Proxy-*Kommunikationsprofil* bzw. die Adresse des Kommunikationspartners im WAN, zu dem ein TLS-Proxy-Kanal aufgebaut werden soll.
Semantic Versioning 2.0.0	Versionierungsschema für Versionen in Form MAJOR.MINOR.PATCH mit wohldefinierter Semantik. Beschrieben in [SemVer].
ServerNameIndication	Eine Erweiterung des TLS-Protokolls, durch die der Client dem Server anzeigt, zu welchen Hostnamen er einen TLS-Verbindungsaufbau initiieren möchte.
SMGW-ID	Identifiziert das SMGW eindeutig in der SM-PKI und entspricht dem Namen des Inhabers der SMGW-Zertifikate (GW_WAN_SIG_CRT, GW_WAN_ENC_CRT, GW_WAN_TLS_CRT). Die "SMGW-ID" wird nach [SM-PKI-CP] Anhang A für das SMGW basierend auf der *kanonisierten Form* der herstellerübergreifend eindeutigen Geräteidentifikation nach [DIN43849] gebildet.
SubjectCN	Das "commonName" Attribut des X.520 "distinguishedName" Attributes des "Subject"-Datenfeldes eines X.509-Zertifikates. Enthält den Namen des Zertifikatsinhabers.
SubjectDN	X.520 "distinguishedName" Attributes des "Subject"-Datenfeldes eines X.509-Zertifikates. Enthält den Namen des Zertifikatsinhabers und ggf. weitere Attribute wie Sequenznummer und Organisation.
technische Einrichtung	Im Kontext dieser TR ein Gerät oder eine Anlage, die über einen CLS-Kommunikationsadapter informationstechnisch an das SMGW anbindbar ist. Dies schließt fernsteuerbare Verbrauchs- und Erzeugungseinrichtungen gemäß [MsbG], [EEG], [EnWG], Steuerungseinrichtungen und Ausstattungen zur Verbrauchsabrechnung ein.
TLS-Proxy-Funktion	Vom SMGW für eine Komponente im HAN des SMGW und einen Kommunikationspartner im WAN des SMGW bereitgestellte Funktionalität zu Aufbau und Nutzung eines *TLS-Proxy-Kanals*.

TLS-Proxy-Kanal	Ein vom SMGW vermittelter TLS-gesicherter Kommunikationskanal zwischen einer Komponente im HAN des SMGW und einem Kommunikationspartner im WAN des SMGW, der durch eine *TLS-Proxy-Funktion* realisiert ist. Dazu wird eine *TLS-Verbindung* zwischen SMGW und Kommunikationspartner im WAN sowie zwischen SMGW und Komponente im HAN des SMGW aufgebaut. Die übertragenen Anwendungsinformationen werden nicht durch den Proxy (bzw. das SMGW) verarbeitet, verändert oder persistiert.
TLS-Verbindung	Eine über eine TLS-Session abgesicherte bidirektionale Transportverbindung zwischen zwei Kommunikationspartnern.
Vertrauensanker	Trust Anchor gemäß RFC5280 Kapitel 6
Weitverkehrsnetz	Kommunikationsnetzwerk mit beliebig großer räumlicher Ausdehnung, z.B. das Internet.

Literaturverzeichnis

[AIS B1] *AIS B1, Version 1.2: Requirements for ST and IAR.* Bundesamt für Sicherheit in der Informationstechnik. 2023.

[AIS B2] *AIS B2, Version 1.2: Requirements for the evaluation of cryptographic mechanisms according to the BSZ.* Bundesamt für Sicherheit in der Informationstechnik. 2023.

[AIS B3] *AIS B3, Version 1.2: Requirements for user guidance.* Bundesamt für Sicherheit in der Informationstechnik. 2023.

[BSZ-Produkte] Bundesamt für Sicherheit in der Informationstechnik. *BSZ-Produkte, v.1.2: Produktzertifizierung: Programm Beschleunigte Sicherheitszertifizierung (BSZ).* 2023.

[DIN43849] *DIN43849 (Bisher DIN 43863-5:2012-04) Messeinrichtungen und systeme, sowie Zusatzeinrichtungen und Steuergeräte – Herstellerübergreifende Identifikationsnummer.* 2023. VDE|DKE K461.

[DS] *Detailspezifikationen zur TR-03109-5 - Anforderungen an die Interoperabilität eines CLS-Kommunikationsadapters.* 2023. Bundesamt für Sicherheit in der Informationstechnik.

[EEG] *Gesetz für den Ausbau erneuerbarer Energien (Erneuerbare-Energien-Gesetz — EEG).*

[EnWG] *Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz — EnWG).*

[GNDEW] *Gesetz zum Neustart der Digitalisierung der Energiewende (GNDEW).*

[Herstellererklärung] *Herstellererklärung zur Einhaltung des Standes der Technik nach § 22 Absatz 2 MsbG: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/Kommunikationsadapter/kommunikationsadapter_node.html.* Bundesamt für Sicherheit in der Informationstechnik.

[MsbG] *Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz - MsbG).* Bundesministerium für Wirtschaft und Energie.

[PP-0073] *BSI-CC-PP-0073-2014, v1.3.1 Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP).* 2022. Bundesamt für Sicherheit in der Informationstechnik.

[PP-0077] *BSI-CC-PP-0077-2014, v1.3 Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP).* 2014. Bundesamt für Sicherheit in der Informationstechnik.

[RFC0791] *INTERNET PROTOCOL (IPv4).* IETF. September 1981.

[RFC0792] *INTERNET CONTROL MESSAGE PROTOCOL (ICMP).* IETF. September 1981.

[RFC1035] *Domain names - implementation and specification.* IETF und P. Mockapetris. 1987.

[RFC1122] *Requirements for Internet Hosts -- Communication Layers.* IETF. Oktober 1989.

[RFC2119] *Key words for use in RFCs to Indicate Requirement Levels.* IETF und Scott Bradner. 1997.

[RFC3927] *Dynamic Configuration of IPv4 Link-Local Addresses.* IETF. Mai 2005.

[RFC4443] *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification.* IETF. March 2006.

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

[RFC5905] *Network Time Protocol Version 4: Protocol and Algorithms Specification.* IETF, D. Mills, J. Martin, J. Burbank und W. Kasch. 2010.

[RFC5915] *Elliptic Curve Private Key Structure.* IETF, S. Turner und D. Brown. 2010.

[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.

[RFC6918] *Formally Deprecating Some ICMPv4 Message Types.* IETF. April 2013.

[RFC8200] *Internet Protocol, Version 6 (IPv6) Specification.* IETF. July 2017.

[RFC8504] *IPv6 Node Requirements.* IETF. January 2019.

[RFC9293] *Transmission Control Protocol (TCP).* IETF. August 2022.

[SemVer] *Semantic Versioning 2.0.0.* semver.org [https://semver.org]

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

[SOGIS-Crypto] *SOG-IS Crypto Evaluation Scheme; Agreed Cryptographic Mechanisms.* Regelmäßig aktualisiert.

[TR-02102-1] *BSI TR-02102-1: Kryptographische Verfahren und Schlüssellängen.* Regelmäßig aktualisiert. Bundesamt für Sicherheit in der Informationstechnik.

[TR-02102-2] *Technische Richtlinie BSI-TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security*. Regelmäßig aktualisiert. Bundesamt für Sicherheit in der Informationstechnik.

[TR-02102-3] *Technische Richtlinie BSI-TR-02102-3 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 3 - Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2).* Regelmäßig aktualisiert. Bundesamt für Sicherheit in der Informationstechnik.

[TR-02102-4] *Technische Richtlinie BSI-TR-02102-4 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 4 – Verwendung von Secure Shell (SSH).* Regelmäßig aktualisiert. Bundesamt für Sicherheit in der Informationstechnik.

[TR-03109] *Technische Richtlinie TR-03109, v.1.1: Dachdokument.* 2021. Bundesamt für Sicherheit in der Informationstechnik.

[TR-03109-1] *Technische Richtlinie TR-03109-1, v.1.1.1: Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems.* 2021. 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-03116-4] *BSI TR-03116-4: Kryptographische Vorgaben für Projekte der Bundesregierung Teil 4 - Kommunikationsverfahren in Anwendungen.* Regelmäßig aktualisiert. Bundesamt für Sicherheit in der Informationstechnik.

[TR-Produkte] *Produktzertifizierungssystem Technische Richtlinien.* Regelmäßig aktualisiert. Bundesamt für Sicherheit in der Informationstechnik.

[VDE-AR-E 2829-6-1] VDE. *Technischer Informationsaustausch an der Schnittstelle zur Liegenschaft und den darin befindlichen Elementen der Kundenanlagen - Teil 6-1: Use Cases.* 2022-12.

[VDE-AR-E 2829-6-4] VDE. *Technischer Informationsaustausch an der Schnittstelle zur Liegenschaft und den darin befindlichen Elementen der Kundenanlagen - Teil 6-4: SHIP.* 2023-09.

[X.690] *ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).* 07/2002. ITU.

Anhang A Abkürzungsverzeichnis

Abkürzung	Beschreibung
aEMT	Aktiver Externer Marktteilnehmer
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSZ	Beschleunigte Sicherheitszertifizierung
CA	Certification Authority
CLS	Controllable Local System
CON	Consumer bzw. Anschlussnutzer
DS	Detailspezifikation
EMT	Externer Marktteilnehmer
EnWG	Energiewirtschaftsgesetz
FA	Fachlicher Anwendungsfall
GWA	Smart-Meter-Gateway-Administrator
HAN	Home Area Network gemäß [PP-0073]
HKS	HAN-Kommunikationsszenario
HTTP	HyperText Transfer Protocol
ICS	Implementation Conformance Statement
IETF	Internet Engineering Task Force
IOP	Interoperabilität
IP	Internet Protocol
ITS	IT-Sicherheit
KS	Kommunikationsszenario
LMN	Local Metrological Network gemäß [PP-0073]
MessEG	Mess- und Eichgesetz
MessEV	Mess- und Eichverordnung
MSB	Messstellenbetreiber
MsbG	Messstellenbetriebsgesetz
N/A	Nicht anwendbar
NTP	Network Time Protocol
REQ	Requirement
RFC	Request For Comments
RTT	Round Trip Time
SM-PKI	Smart-Meter - Public Key Infrastructure
SMGW	Smart-Meter-Gateway
SNI	Server Name Indication des TLS-Protokolls
ST	Security Target
TA	Technischer Anwendungsfall
TCP	Transmission Control Procotol des Internet-Protokolls
TLS	Transport Layer Security, Transportsicherungsprotokoll
TR	Technische Richtlinie(n) des Bundesamtes für Sicherheit in der Informationstechnik – im Sinne dieses Dokuments BSI TR-03109-5

Abkürzung	Beschreibung
TS	Testspezifikation zu einer Technischen Richtlinie
UDP	User Datagram Protocol des Internet-Protokolls
UTC	Coordinated Universal Time, Zeitskala
WAN	Wide Area Network gemäß [PP-0073]

Tabelle A.1 In der TR verwendete Abkürzungen

Anforderungsverzeichnis

ICS-Anforderungen