Bundesamt
für Sicherheit in der
Informationstechnik

Technische Richtlinie BSI TR-03109

Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen

Version 0.20, Datum 10.10.2011

Bundesamt für Sicherheit in der Informationstechnik

Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-100

E-Mail: smartmeter@bsi.bund.de
Internet: https://www.bsi.bund.de

Vorwort des Präsidenten

Vorwort

Danksagung

Danksagung

Inhaltsverzeichnis

Anhänge

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Zielsetzung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat diese Technische Richtlinie (TR) erstellt mit dem Ziel, Anforderungen an die Funktionalität, Interoperabilität und Sicherheit, die eine Kommunikationseinheit eines intelligenten Messsystems erfüllen muss, zu beschreiben.

Die Technische Richtlinie referenziert und ergänzt das Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems [GW_PP], indem die funktionalen Sicherheitsanforderungen an diese Komponente und ihre Einsatzumgebung u.a. um Vorgaben an Kommunikationsprotokolle, Tarif- und Berechtigungsprofile und kryptographische Verfahren erweitert werden.

1.2 Zielgruppe

Die Technische Richtlinie richtet sich in erster Linie an Hersteller von Kommunikationseinheiten intelligenter Messsysteme ("Smart Meter Gateways"). Die Konformität eines Produktes zu den Anforderungen dieser TR wird durch eine Prüfung bei einer für diese Thematik anerkannten Prüfstelle bescheinigt und durch ein Zertifikat des BSI abschließend bestätigt. Hierzu existiert eine entsprechende Verfahrensbeschreibung [in Arbeit], in der die einzelnen Schritte zur Erlangung eines solchen Zertifikats dargelegt werden.

1.3 Anwendungsbereich

Die Technische Richtlinie betrachtet Smart Meter Gateways, die im Kontext des Smart Metering / Smart Grid genutzt werden.

1.4 Fachlich zuständige Stelle

Fachlich zuständig für die Fortentwicklung des Dokumentes „Technische Richtlinie BSI TR-03109: Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen“ ist das Bundesamt für Sicherheit in der Informationstechnik.

Anschrift: Bundesamt für Sicherheit in der Informationstechnik
Abteilung S
Postfach 20 03 63
53133 Bonn

1.5 Terminologie

Für die genauere Unterscheidung zwischen normativen und informativen Inhalten werden die dem [RFC2119] entsprechenden in Großbuchstaben geschriebenen, deutschen Schlüsselworte verwendet:

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

Die Kapitel der Technischen Richtlinie sind grundsätzlich als normativ anzusehen. Informative Kapitel werden explizit gekennzeichnet.

1.6 Aufbau der Technischen Richtlinie

Beginnend mit Kapitel 2 „Technische Einleitung“ wird mit einer kurzen Darstellung gezeigt, wie die Einbettung des Smart Meter Gateways (SM-GW) in die Gesamtarchitektur eines Smart Metering Systems zu sehen ist. Darauf aufbauend werden die funktionalen Aspekte des Smart Meter Gateways skizziert. Zuvor werden die Marktteilnehmer benannt, die in verschiedenen Rollen mit dem Smart Meter Gateway kommunizieren können.

Das folgende Kapitel 3 „Anforderungen an die Kommunikationsverbindungen und Protokolle des Smart Meter Gateways“ macht Vorgaben zur Sicherung aller Kommunikationsbeziehungen des Smart Meter Gateways und stellt Mindestforderungen in Bezug auf die zu unterstützenden Applikationsprotokolle.

Kapitel 4 beschreibt die „Tarifprofile und Tarifierung“, sowie die Berechtigungsprofile mit deren Hilfe das Rollen- und Rechtemanagement zum Zugriff auf die Messwerte im Smart Meter Gateway festgelegt wird.

In Kapitel 5 „Weitere Funktionale Anforderungen“ werden Anforderungen an das Smart Meter Gateway spezifiziert (z.B. das Logdaten-Format, notwendige Administrationsbefehle, etc.) die neben den in Kapitel 4 dargestellten Funktionen wichtig sind. Nicht-funktionale Anforderungen bzw. Eigenschaften, die das Smart Meter Gateway aufweisen muss, finden sich dann in Kapitel 6.

Sicherheitstechnische Anforderungen an den Betreiber der Smart Meter Infrastruktur sowie die notwendigen Betriebsprozesse werden in Kapitel 7 behandelt.

Anhang A macht Vorgaben an die einzusetzenden kryptographischen Verfahren. Anhang B beschreibt das Sicherheitsmodul und die von ihm bereitzustellende Funktionalität und Anhang C definiert die den Sicherheitsmechanismen zugrunde liegende Zertifikatsinfrastruktur und die dort ablaufenden Prozesse.

171 ## 1.7 Versionshistorie

Version	Datum	Beschreibung
0.20	10.10.2011	Veröffentlichung Draft 1

172

2 Technische Einleitung

Dieses Kapitel hat informativen Charakter.

Ziel dieses Kapitels ist es, die Einbettung der Kommunikationseinheit eines intelligenten Messsystems, deren Sicherheitsanforderungen im Schutzprofil [GW_PP] spezifiziert sind, in sein technisches und organisatorisches Umfeld zu beschreiben. Diese Kommunikationseinheit wird im Folgenden mit dem englischen Terminus „Smart Meter Gateway“ bezeichnet.

Dabei wird nach einer kurzen Erläuterung der Zielsetzung von Smart Metering beschrieben, welche Marktteilnehmer in welchen Rollen und mit welchen Aufgaben an der Kommunikation mit einem Smart Meter Gateway beteiligt sind. Des Weiteren wird die Funktionalität des Smart Meter Gateways, kategorisiert nach seinen externen Schnittstellen, skizziert. Die Schnittstellen sind Netzen zugeordnet, deren Bedeutung erläutert wird. Weitere zentrale Funktionen, die entweder netzwerkübergreifend oder intern im Smart Meter Gateway bereitgestellt werden, sind am Ende des Kapitels aufgeführt.

Dieses Kapitel hat eine einleitende und informative Funktion. Weiterführende Details und Anforderungen, die prüfrelevant sind, werden in den folgenden Kapiteln behandelt, auf die in dieser Einleitung jeweils verwiesen wird.

2.1 Zielsetzung für Smart Metering

HINWEIS: Befindet sich in Arbeit

2.2 Berechtigte Rollen am Smart Meter Gateway

Marktteilnehmer, die mit dem Smart Meter Gateway kommunizieren, agieren dabei in verschiedenen Rollen. Diese natürlichern oder juristischen Personen werden im Energiewirtschaftsgesetz [EnWG §3 Begriffsbestimmungen] bzw. auf den Internetseiten der BNetzA (siehe Rubrik „Startseite → Sachgebiete → Elektrizität/Gas → Glossar“) definiert und ihre Aufgaben werden dort beschrieben.

Das Schutzprofil [GW_PP] unterscheidet zwischen den folgenden Rollen:

Verbraucher

Der Verbraucher ist die natürliche oder juristische Person, die Eigentümer der im Smart Meter Gateway verarbeiteten und gespeicherten Messwerte ist. Anschlussnutzer oder Anschlussnehmer, die Strom, Gas, Wasser oder Wärme verbrauchen, kommunizieren also in ihrer Verbraucherrolle mit dem Smart Meter Gateway.

Externe Marktteilnehmer

Externe Marktteilnehmer sind aus Sicht des Smart Meter Gateways alle Marktteilnehmer im Weitverkehrsnetz, mit denen das Smart Meter Gateway eine Kommunikation zum Austausch von Daten

aufnehmen kann. Hierunter fallen also z.B. der Verteilnetzbetreiber, der Messstellenbetreiber, der Messdienstleister und der Lieferant.

Smart Meter Gateway Administrator

Das Smart Meter Gateway - als neue Komponente im Messstellenbetrieb - fällt in den Verantwortungsbereich des Messstellenbetreibers. Der Messstellenbetreiber ist die vertrauenswürdige Instanz, die das Smart Meter Gateway installiert, konfiguriert, überwacht und steuert. Der Messstellenbetreiber in seiner Rolle als Gateway Administrator (kurz: Administrator) erstellt und administriert die in das Smart Meter Gateway eingespielten Tarif- und Berechtigungsprofile und führt bei Bedarf die Aktualisierung der Smart Meter Gateway-Software durch.

2.3 Funktionalität des Smart Meter Gateways

Die Funktionalität des Smart Meter Gateways wird bestimmt durch seine Rolle als Datenspeicher, Datenaufbereiter und Firewall an der Schnittstelle zwischen dem lokalen Bereich beim Endkunden und der Außenwelt. Abbildung 1 gemäß [GW_PP] zeigt schematisch die verschiedenen Netze, mit denen das Smart Meter Gateway verbunden ist und in denen es seine Funktionen zur Verfügung stellt.

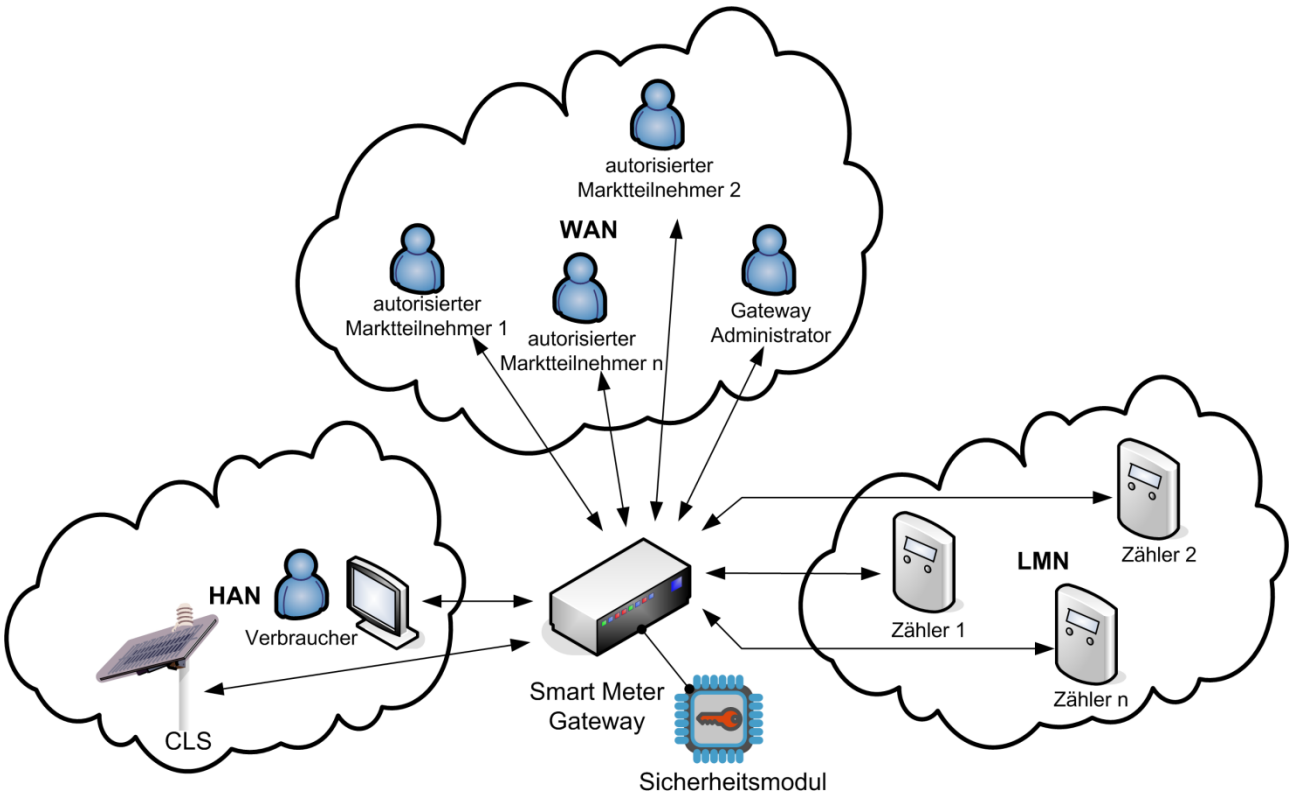


Abbildung 1: Einbettung des Smart Meter Gateways in seine Einsatzumgebung

Das Smart Meter Gateway ist mit den folgenden drei Netzen verbunden:

- Local Metrological Network (LMN),

das lokale metrologische Netz, in dem alle Zähler für Stoff- und Energiemengen (Strom, Gas, Wasser, Wärme) eines Haushaltes oder mehrerer Mietparteien subsumiert werden.

- Wide Area Network (WAN),

  das Weitverkehrsnetz, über das die Kommunikation mit den externen Marktteilnehmern und insbesondere auch mit dem Smart Meter Gateway Administrator etabliert wird.

- Home Area Network (HAN),

  das lokale Netz beim Anschlussnutzer, in dem die steuerbaren Verbraucher bzw. Erzeuger (CLS Controllable Local Systems, z.B. KWK-/Photovoltaik-Anlagen) sowie die mit dem Smart Meter Gateway verbundene Anzeigeeinheit zu finden sind.

Das Smart Meter Gateway ist die Kommunikationseinheit vor Ort beim Verbraucher und dient als zentrale Einheit zur Protokoll- und Datenumwandlung. Es agiert gleichzeitig als Filter, um die einzelnen Netze zu separieren.

2.3.1 Smart Meter Gateway Funktionen für das lokale metrologische Netz

Das Smart Meter Gateway kommuniziert mit den elektronischen Zählern im lokalen metrologischen Netz und ist für die Erfassung, Verarbeitung und Speicherung von Messwerten und ggf. Netzstatuswerten verantwortlich.

Die sichere Kommunikation mit den Zählern erfolgt mit Hilfe der in Kapitel 3.3 festgelegten Protokolle.

Erfassung, Zeitstempelung, Tarifierung und Speicherung von Messwerten

Die von den Zählern im LMN übermittelten Daten können sowohl Verbrauchswerte als auch Angaben über in das Netz eingespeiste Energiemengen (z.B. bei Photovoltaikanlage, Blockheizkraftwerk) sein. Zusätzlich können auch weitere lokal gemessene Netzparameter wie z.B. Netzspannung, Frequenz, Phasenwinkel etc. von den Zählern bereitgestellt werden. Folgende Prozessschritte müssen vom Smart Meter Gateway an der LMN Schnittstelle erbracht werden:

1) Das Smart Meter Gateway empfängt oder erfragt in regelmäßigen, vom Gateway Administrator konfigurierbaren, Zeitabständen (bspw. alle 15 Minuten) die Messwerte der lokal angeschlossenen Zähler für Stoff- und Energiemengen.
2) Nach erfolgreicher Entschlüsselung und Integritätsprüfung der Messwerte versieht das Smart Meter Gateway die Verbrauchswerte mit einem Zeitstempel, der von der Systemuhr des Gateways geliefert wird.
3) Das Smart Meter Gateway ordnet den mit einer Zeit versehenen Messwerten die gültige Tarifstufe zu, die aus dem Tarifprofil ermittelbar ist, welches dem Zähler zugeordnet ist. Dieser Datensatz wird dann zur weiteren Verarbeitung abgespeichert.

Der Vorgang der Zuordnung eines Messwertes zu einer Tarifstufe wird in dieser TR als Tarifierung bezeichnet (siehe dazu auch Kapitel 4).

Die weiteren Verarbeitungsschritte für den gespeicherten Datensatz richten sich nach den Berechtigungsprofilen, die für diese Klasse von Messwerten im Smart Meter Gateway hinterlegt wurden.

Das Smart Meter Gateway unterliegt wegen der durchgeführten Zeitstempelung und Tarifierung der Messwerte der Eichpflicht.

2.3.2 Smart Meter Gateway Funktionen im Weitverkehrsnetz

Die Verbindung des Smart Meter Gateways mit den Marktteilnehmern geschieht über eine WAN Verbindung (z.B. als GSM/GPRS oder DSL Anschluss).

Die Absicherung der Kommunikation erfolgt mittels der in Kapitel 3.2 festgelegten Protokolle.

Das Smart Meter Gateway besitzt im WAN eine vertrauenswürdige Instanz, den Gateway Administrator (siehe Kapitel 2.2), der das Smart Meter Gateway administriert und wartet.

Folgende Funktionen des Smart Meter Gateways müssen über die WAN-Schnittstelle realisiert werden:

Verarbeitung und Übertragung der Messwerte anhand von Berechtigungsprofilen

Im Smart Meter Gateway werden vom Gateway Administrator für jeden angeschlossenen Zähler (d.h. für jede Klasse von Messdaten) Berechtigungsprofile hinterlegt (siehe Kapitel 4.3 und Kapitel 1.4.6.1 in [GW-PP]). Diese legen fest, welche Aktionen und Operationen mit den empfangenen Messwerten des jeweiligen Zählers durchgeführt werden dürfen. Diese Profile modellieren die vertraglichen Vereinbarungen des Anschlussnutzers mit seinen Vertragspartnern in Bezug auf die gemessenen Zählerwerte.

Empfang von Administrations- und Konfigurationsinformationen

Das Smart Meter Gateway muss die vom Gateway Administrator gesendeten Befehle, Parameter oder Konfigurationsinformationen empfangen und verarbeiten, z.B.:

- ***Tarifinformationen***

  Zur Abbildung von tageszeitabhängigen oder lastvariablen Tarifen übermittelt der Gateway Administrator Tarifinformationen (siehe Kapitel 4.2) an das Smart Meter Gateway, die er vom zugehörigen Energielieferanten erhalten hat. Die Tarifinformationen werden im Smart Meter Gateway gespeichert und dienen zur Zuordnung von empfangenen Messwerten zu entsprechenden (z.B. tageszeitabhängigen) Tarifstufen.

- ***Berechtigungsprofile***

  Die Berechtigungsprofile, durch die die Aktionen des Smart Meter Gateways konfiguriert und gesteuert werden, werden vom Gateway Administrator in einer Datenstruktur (siehe Kapitel 4.3) erfasst und mittels kryptographischer Verfahren gesichert an das Smart Meter Gateway übertragen.

- ***Software Update***

  Ein Update der Software des Smart Meter Gateways ist möglich. Den Befehl dazu erhält das Smart Meter Gateway vom Gateway Administrator. Daraufhin lädt das Smart Meter Gateway die neue Software über eine verschlüsselte und authentifizierte Verbindung von einem Update Server herunter und aktiviert die neue Firmware. Die Applikationsdaten im Smart Meter Gateway (z.B. Messwerte, Zählerprofile, Tarifprofile, Berechtigungsprofile) dürfen durch ein Software Update nicht verändert oder gelöscht werden. Der Updateprozess selbst muss „fail safe“ implementiert sein, so dass Prozessfehler nicht zum Ausfall des Gateways führen.

  HINWEIS: Ablauf und Relevanz bzgl. Eichrecht werden zur Zeit untersucht und abgestimmt.

Das Smart Meter Gateway lehnt Verbindungsaufbauwünsche aus dem WAN ab. Es kann aber selbst regelmäßig eine (TLS-) Verbindung zu seinem Gateway Administrator aufbauen, um Befehle entgegennehmen zu können. Alternativ kann es eine aufgebaute Verbindung permanent offen halten oder auch durch ein Wake-Up Mechanismus zum Verbindungsaufbau aufgefordert werden.

Wake-Up-Service

Die im Schutzprofil definierten Mindestanforderungen sehen vor, dass das Smart Meter Gateway nach außen hin 'unsichtbar' ist. Es stellt somit keine Dienste an der WAN-Schnittstelle zur Verfügung.

Das Smart Meter Gateway kann aber dennoch von außen mithilfe des Wake-Up-Service zu einer Reaktion veranlasst werden. Beim Wake-Up-Service empfängt das Smart Meter Gateway ein spezielles vom Gateway Administrator signiertes Datenpaket (siehe Kapitel 3.2.5). Nach erfolgreicher Verifikation dieses einzelnen Paketes baut das Smart Meter Gateway eine TLS Verbindung zum Gateway Administrator auf. Dieser kann über die nun etablierte Verbindung weitere Administrationsbefehle ausführen.

Der Wake-Up-Service muss als Teilprozess im Smart Meter Gateway so implementiert sein, dass dessen Ausführungspriorität niedriger ist als die der regulären Prozesse zur Messdatenverarbeitung. Der wiederholte Aufruf des Dienstes (z.B. als „denial of service“ Attacke) darf die normalen Dienstleistungen des Smart Meter Gateways nie vollständig blockieren.

2.3.3 Smart Meter Gateway Funktionen für das Home Area Network

Das Smart Meter Gateway stellt zwei logische Schnittstellen im HAN bereit. Über die erste können lokale Erzeuger oder intelligente Endgeräte (CLS, Controllable Local Systems) gesteuert werden. Die zweite dient dazu, Verbrauchswerte und andere Informationen individuell für jeden Anschlussnutzer abrufbar zu machen.

CLS-Schnittstelle

Über die CLS-Schnittstelle des Smart Meter Gateways können steuerbare Komponenten im HAN des Anschlussnutzers (z.B. intelligente Hausgeräte, Photovoltaikanlagen, Klimaanlagen) gesicherte Kommunikationsverbindungen ins WAN zu externen Dienstleistern aufbauen (siehe [GW-PP] Kapitel 1.4.6.4). Das Smart Meter Gateway stellt dazu seine TLS Funktionalität zur Verfügung. Die dann über diese TLS Verbindung ablaufende Kommunikation und die dazugehörigen Protokolle, die dem Monitoring oder der Steuerung der CLS-Komponente dienen, sind für das Smart Meter Gateway transparent.

Schnittstelle für Anzeigeeinheiten

Das Smart Meter Gateway bietet dem Anschlussnutzer mit Hilfe der logischen Schnittstelle für Anzeigeeinheiten die Möglichkeit im Smart Meter Gateway gespeicherte Informationen im HAN abzurufen. Auf diese Daten ist nur ein lesender Zugriff nach erfolgreicher Authentifizierung des Anschlussnutzers möglich. Eine Anzeigeeinheit kann ein dediziertes, kryptographisch gesichertes Display, ein lokaler PC oder ein anderes Gerät im HAN Bereich sein, welches den kryptographisch gesicherten Datenstrom verarbeiten kann. Es können nur die Daten eingesehen werden, die im Smart Meter Gateway dem authentifizierten Benutzer zugeordnet sind.

Mindestens folgende Informationen stellt das Smart Meter Gateway an der Schnittstelle für Anzeigeeinheiten bereit:

- *Eichrechtliche relevante Daten*

  Dies sind alle zur Nachprüfung einer Abrechnung notwendigen Verbrauchs- bzw. Einspeisewerte und die zugrundeliegenden Tarifinformationen.

- *Daten zum Informationsfluss*

  Dies betrifft Log-Informationen über die vom Smart Meter Gateway aufgebauten Verbindungen zu den externen Marktteilnehmern. Zusammen mit den Berechtigungsprofilen kann der Anschlussnutzer damit verifizieren, dass nur Datenübertragungen stattfinden, die vertragliche vereinbart sind.

- *Feingranulare Verbrauchswerte*

  Feingranulare Messwerte, die im Smart Meter Gateway gesammelt werden. Sie können dem Kunden zur Visualisierung seines Energieverbrauches dienen und bieten ihm damit die Grundlage, seinen Verbrauch zu optimieren (siehe Kapitel 3.4.2).

2.3.4 Weitere Funktionen des Smart Meter Gateways

Neben den bereits genannten Funktionalitäten des Smart Meter Gateways, gibt es weitere Funktionen, die vom Smart Meter Gateway erbracht werden müssen.

Nutzerverwaltung/Mandantenfähigkeit

Das Smart Meter Gateway erfasst und speichert die Messwerte von Zählern verschiedener Anschlussnutzer (bspw. in Mehrfamilienhäusern). Dazu muss das Smart Meter Gateway Mechanismen

implementieren, um die Multi-Mandantenfähigkeit und die Authentifizierungsanforderungen (siehe [GW_PP] Kapitel 1.4.6.6) umsetzen zu können. Pro Anschlussnutzer ist nur ein Account vorzusehen. Separate Benutzerkennungen, unterhalb der Ebene des Anschlussnutzers, sind nicht vorgesehen.

Zeitservice

Das Smart Meter Gateway stellt eine gültige, vertrauenswürdige Uhrzeit bereit. Dazu muss das Smart Meter Gateway über ein Uhrwerk (Gateway-Clock) mit Gangreserve und Synchronisationsfunktion verfügen. Mit einer vertrauenswürdigen Zeitquelle wird das Smart Meter Gateway in die Lage versetzt, Messwerte mit einem zuverlässigen Zeitstempel zu versehen. Hierbei darf die Gateway-Clock nicht zu sehr von einer amtlichen Zeit abweichen und muss deswegen regelmäßig synchronisiert werden.

Die Synchronisation der Gateway-Clock mit einer zuverlässigen externen Zeitquelle geschieht gemäß den Vorgaben aus Kapitel 3.2.5.

Kryptographische Funktionen

Zur Erfüllung kryptographischer Funktionen wie Ver- und Entschlüsselung von Daten, Signaturerzeugung, Signaturprüfung und Generierung von Schlüsseln bedient sich das Smart Meter Gateway eines nach Common Criteria (siehe [SM_PP]) zertifizierten Sicherheitsmoduls. Das Sicherheitsmodul stellt dabei u.a. folgende Dienste zur Verfügung (siehe auch [GW_PP] Kapitel 1.4.8):

- Bereitstellung der Identität des Smart Meter Gateways durch die sichere Speicherung privater Schlüssel des Smart Meter Gateways
- Funktionen zur asymmetrischen Kryptographie und Erzeugung von Zufallszahlen

Das Sicherheitsmodul muss die Anforderungen aus Anhang A erfüllen.

Protokollierung

Das Smart Meter Gateway protokolliert seine Aktionen in drei unterschiedlichen Log-Bereichen, im System-Log, Kunden-Log sowie im eichtechnischen Logbuch (siehe [GW_PP] Kapitel 4.1).

- *System-Log*

  Jedes wichtige Event (z.B. Fehlermeldungen, Ausfall der WAN Verbindung, sicherheitsrelevante Ereignisse etc.) im Smart Meter Gateway wird in einem System-Log protokolliert. Dieses Log kann nur von dem autorisierten Gateway Administrator eingesehen werden. Die Informationen dienen dazu, den momentanen Status des Smart Meter Gateways zu erkennen und eventuelle Fehlerquellen oder Störungen zu identifizieren.

- *Kunden-Log*

  Alle Transaktionen des Smart Meter Gateways, z.B. das Versenden von Messwerten, und Aktivitäten des Gateway Administrators werden in einem Kunden-Log festgehalten. Ein authentifizierter und autorisierter Anschlussnutzer kann diese Informationen vom Smart Meter Gateway über die logische Display-Schnittstelle abrufen und somit nachverfolgen, wer, wann, welche Daten erhalten hat. Hier müssen außerdem alle abrechnungsrelevanten Informationen aufgezeichnet werden.

Zur Wahrung der Vertraulichkeit und Integrität der personenbezogenen Protokolldaten ist einem Gateway Administrator der Zugriff auf das Kunden-Log nicht erlaubt.

- *Eichtechnisches Log*

  Im eichrechtlichen Logbuch werden eichtechnisch relevante Ereignisse (z.B. erkannte Verfälschungen von Messungen, fehlgeschlagene Zeitsynchronisierungen) aufgezeichnet. Außerdem erfolgt hier die Registrierung von Änderungen an eichrechtlich relevanten Parametern (z.B. das Stellen der Geräteuhr). Dieses Log kann nur von dem autorisierten Gateway Administrator eingesehen werden.

Aufbau und syntaktische Struktur der Logfiles werden in Kapitel 5 festgelegt.

Pseudonymisierung

Bei der Übertragung von nicht abrechnungsrelevanten Messwerten vom Smart Meter Gateway an einen Marktteilnehmer muss die Identität des Anschlussnutzers (hier gegeben durch die Identität des messenden Zählers) nicht offengelegt werden. Um dies zu erreichen, wird die im Datensatz enthaltene Identifikation des Zählers durch ein Pseudonym ersetzt. Damit auch die Identität des sendenden Gateways unerkannt bleibt, müssen die Daten zusätzlich über einen Dritten (z.B: den Messstellenbetreiber) an den Endempfänger vermittelt werden.

Die Pseudonymisierung im Smart Meter Gateway geschieht durch die beiden folgenden Schritte:

1. Aus Messwerten, die einem Berechtigungsprofil folgend pseudonymisiert übertragen werden sollen, wird die eindeutige Zähler-ID durch das Smart Meter Gateway entfernt und durch ein im Berechtigungsprofil hinterlegtes Pseudonym ersetzt. Die so aufbereiteten Daten werden dann vom Smart Meter Gateway für den Empfänger verschlüsselt, signiert und an den Messstellenbetreiber übertragen.
2. Der Messstellenbetreiber prüft die Signatur des Smart Meter Gateways und damit die Authentizität der empfangenen Daten und leitet diese nach Entfernung der Smart Meter Gateway Signatur an den Empfänger weiter. Damit ist die Rückverfolgung des Anschlussnutzers über das sendende Smart Meter Gateway für den Empfänger unmöglich. Der Empfänger entschlüsselt die Messdaten. Diese enthalten nur ein Pseudonym anstelle der Zähler-ID. Damit ist die Rückverfolgung des Anschlussnutzers über die Zähler-ID unmöglich.

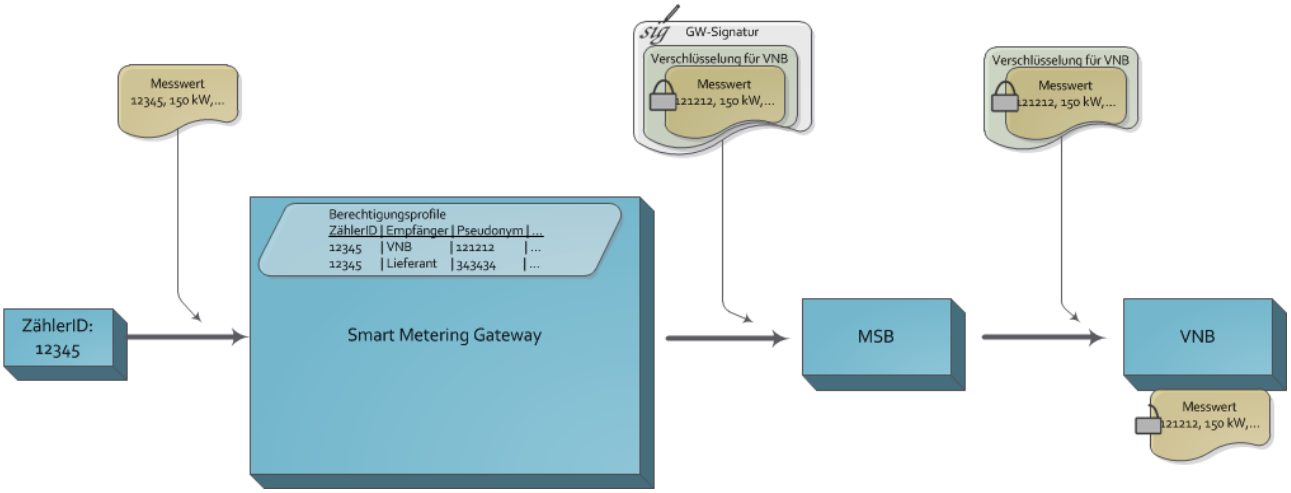


Abbildung 2: Pseudonymisierte Messdatenübertragung

Wenn beispielsweise die Smart Meter Gateways aller Haushalte mit Anschluss an derselben Ortsnetzstation im Berechtigungsprofil zur Übertragung der Messdaten an den Verteilnetzbetreiber dasselbe Pseudonym eingetragen haben, erlauben die so pseudonymisiert übermittelten Messwerte zwar die Bildung eines Lastprofils über ein gesamtes Netzsegment, sie lassen jedoch keine Rückschlüsse auf einen einzelnen Haushalt zu.

3 Anforderungen an die Kommunikationsverbindungen und Protokolle des Smart Meter Gateways

3.1 Einleitung

Dieses Kapitel hat informativen Charakter.

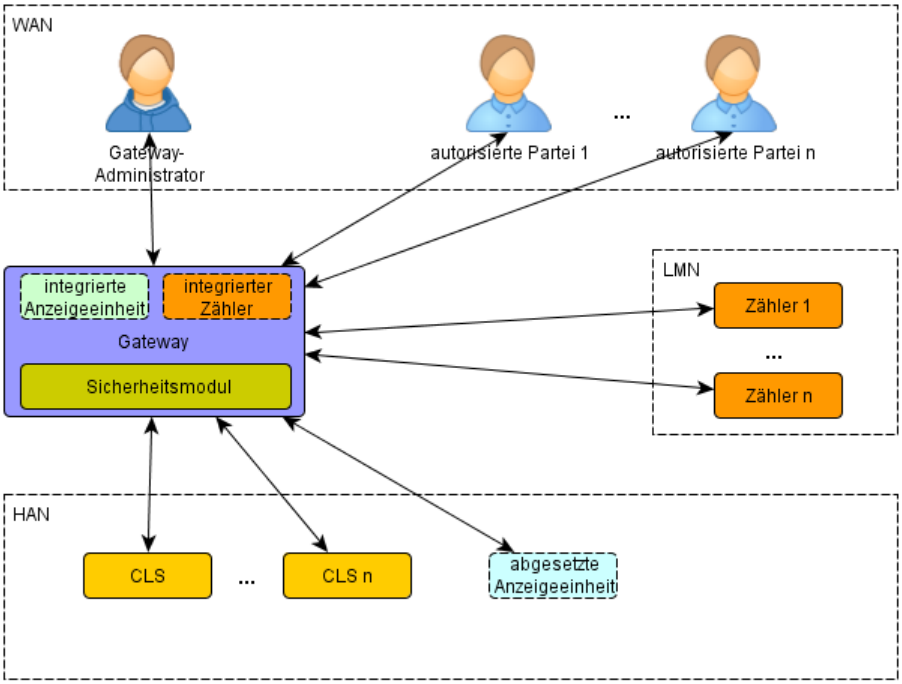


Abbildung 3: Kommunikationsverbindungen des Smart Meter Gateways

Das Smart Meter Gateway verfügt über logische Schnittstellen, um mit unterschiedlichen Parteien und Geräten zu kommunizieren.

Abbildung 3 zeigt eine Übersicht über diese Kommunikationsverbindungen zu den verschiedenen Netzen, an die das Gateway angebunden ist.

Die folgenden Kapitel legen die Anforderungen an die Kommunikation zu den verschiedenen Parteien und Komponenten in den aufgeführten Netzen fest. Neben den Anwendungsprotokollen für die Festlegung der eigentlichen Übertragungen werden dabei auch Maßnahmen zur Sicherung der Kommunikation gefordert.

3.2 Vorgaben an die Kommunikationsverbindungen im WAN

3.2.1 Übersicht

Dieses Kapitel hat informativen Charakter.

Dieses Kapitel definiert die Anforderungen an die WAN-Schnittstelle des Gateways. Das Gateway wird im Betrieb die folgenden Kommunikationsformen über das WAN bereitstellen:

- Sichere Kommunikationsverbindungen zu verschiedenen Teilnehmern im WAN unter Verwendung von TLS und Inhaltsdatenverschlüsselung und -signierung, für die Übermittlung folgender Daten (oder einer Teilmenge davon):
  - Netzstatusdaten (z.B. Auslastung, Phasenwinkel, Frequenz)
  - Abrechnungsrelevante Daten (Verbrauch gemäß Tarif)
- Sichere Kommunikationsverbindungen vom Gateway-Administrator zum Gateway zur Administration, geschützt durch TLS
- Sicherung der CLS-Kommunikation unter Verwendung von TLS (beschrieben in Kapitel 3.4.3)
- Zeitsynchronisation
- Wake-Up Service

Zeitsynchronisation und Wake-Up Service erfolgen gemäß den Vorgaben in Kapiteln 3.2.6 und 3.2.5 und ohne die Verwendung eines bestehenden TLS-Kanals. Alle anderen Kommunikationsverbindungen in das WAN werden über TLS abgesichert, die nur vom Gateway aus hergestellt werden können (siehe hierzu Kapitel 3.2.2.1 und Kapitel 3.4.3).

Der Gateway-Administrator kann eine TLS-Verbindung initiieren, indem er ein Wake-Up-Paket an das Gateway verschickt (s. Kapitel 3.2.5). Das Gateway wird sich daraufhin an die vorkonfigurierte Adresse der zuständigen Partei verbinden.

Das Kapitel 3.2.2.2 definiert die Verschlüsselung und Signatur der eigentlichen Nutzdaten. Diese Nutzdaten können unabhängig vom Betreiber des TLS-Endpunktes an dritte Parteien adressiert sein. In diesem Fall kann der Betreiber des TLS-Endpunktes nur die Signatur des Gateways prüfen und gegebenenfalls entfernen. Die verschlüsselten Daten können dann an die vorgesehene dritte Partei geeignet weiter geleitet werden.

Werden Netzstatusdaten an eine dritte Partei weitergereicht, so wird der Betreiber des Gateway die Signatur entfernen und damit sicherstellen, dass diese Daten nicht auf den eigentlichen Verbraucher zurückgeführt werden können. Sofern notwendig wird das Gateway zudem Daten pseudonymisieren (z.B. IDs).

Oberhalb der Schicht für die Transportsicherung findet sich die Anwendungsschicht, in der Kommunikationsprotokolle für Messdaten (Kapitel 3.2.3) und für die Administration (Kapitel 3.2.4) definiert werden. Die Anwendungsschicht verwendet dabei die Inhaltsdatenverschlüsselung.

Abbildung 4 zeigt die Einordnungen des Kommunikationsmodells im Vergleich zum ISO-Referenzmodell und dem TCP/IP-Modell.

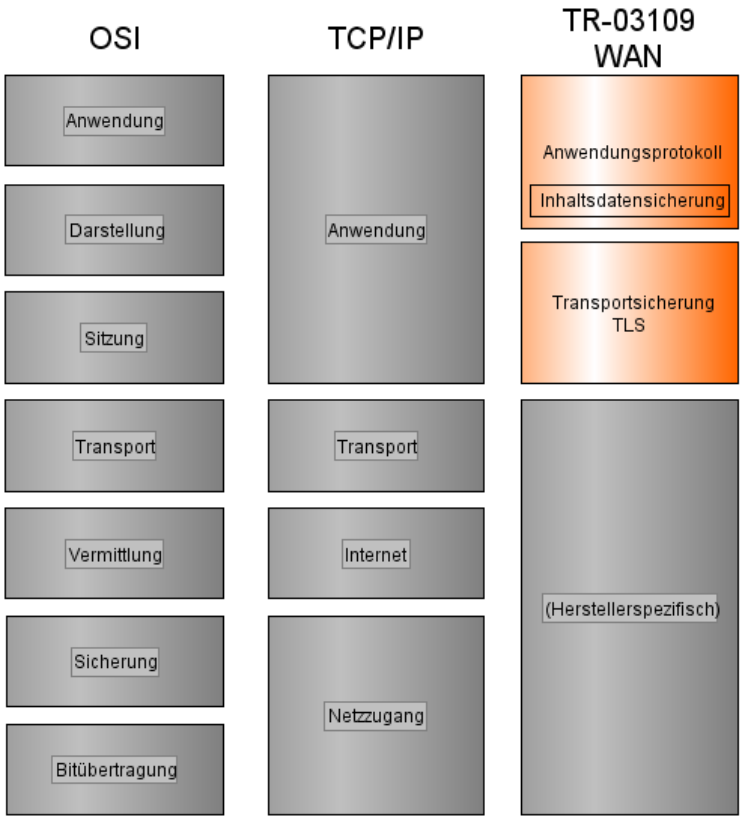


Abbildung 4: Einordnung des Kommunikationsmodells für die Übermittlung von Messwerten und Administrationskommandos im WAN

3.2.2 Sicherung der Kommunikationsverbindungen in das WAN

Die Kommunikationsverbindung in das WAN **MUSS** vom Gateway oberhalb der Transportschicht mittels TLS und auf Inhaltsdatenebene mittels hybrider Verschlüsselung und Signatur abgesichert werden (s. Anhang A).

Mögliche Teilnehmer im WAN sind dabei in Kapitel 2.2 in der Marktteilnehmerübersicht dargestellt.

Die folgenden beiden Unterkapitel 3.2.2.1 und 3.2.2.2 legen die Anforderungen an die TLS-Kommunikation und die Verschlüsselung auf Inhaltsdatenebene fest.

3.2.2.1 Transportsicherung (TLS)

3.2.2.1.1 Allgemeine Anforderungen

Die Implementierung von TLS **MUSS** konform zu [TLS] und [TLS_ECC] sein. Das Gateway **MUSS** die folgende kryptographische Funktionalität umsetzen:

- Generierung von Hashes für Signaturerzeugung und -prüfung
- Symmetrische Ver- und Entschlüsselung nach Aufbau des TLS-Kanals

Die genauen Vorgaben an die Implementierung der kryptografischen Primitive sind in Anhang A definiert und **MÜSSEN** befolgt werden.

Für die Kommunikation mit Teilnehmern im WAN **MUSS** das Gateway in der Rolle eines TLS-Clients einen beidseitig authentifizierten TLS-Kanal aufbauen.

Das Gateway **DARF KEINE** TLS-Verbindungen akzeptieren, die von Teilnehmern aus dem WAN initiiert werden. Das Gateway kann jedoch für einen bestimmten Fall über den Wake-Up-Dienst (s. Kapitel 3.2.5) veranlasst werden, eine Verbindung aufzubauen.

Das notwendige Zertifikat des WAN-Teilnehmers (z.B. MSP_TLS_CERT) **MUSS** zuvor in das Gateway eingebracht worden sein. Das Gateway **MUSS** sicherstellen, dass das von der Gegenseite verwendete Zertifikat dem zuvor eingebrachten entspricht (DIRECT TRUST).

3.2.2.1.2 Anforderungen an die Zusammenarbeit mit dem Sicherheitsmodul

Das Gateway **MUSS** mit einem Sicherheitsmodul zusammenarbeiten, das gemäß [PP_SM] zertifiziert wurde.

Beim Aufbau des TLS-Kanals (Handshake) **MUSS** das Gateway sein Sicherheitsmodul einsetzen, wie in Abbildung 5 und Abbildung 6 beispielhaft dargestellt. Folgende Funktionen des Sicherheitsmoduls **MÜSSEN** verwendet werden:

- Generierung von Zufallszahlen für TLS-Kommando *ClientHello* (GET RANDOM)
- Schlüsselaushandlung des TLS *pre-master secrets* gemäß Diffie-Hellman (NEGOTIATE KEY)
- Signaturerzeugung und –prüfung für Authentifizierung (PSO COMPUTE DIGITAL SIGNATURE, PSO VERIFY DIGITAL SIGNATURE)

Das Gateway ist verantwortlich für die Generierung des *master secrets* und **MUSS** dazu das ausgehandelte *pre-master secret* verwenden.

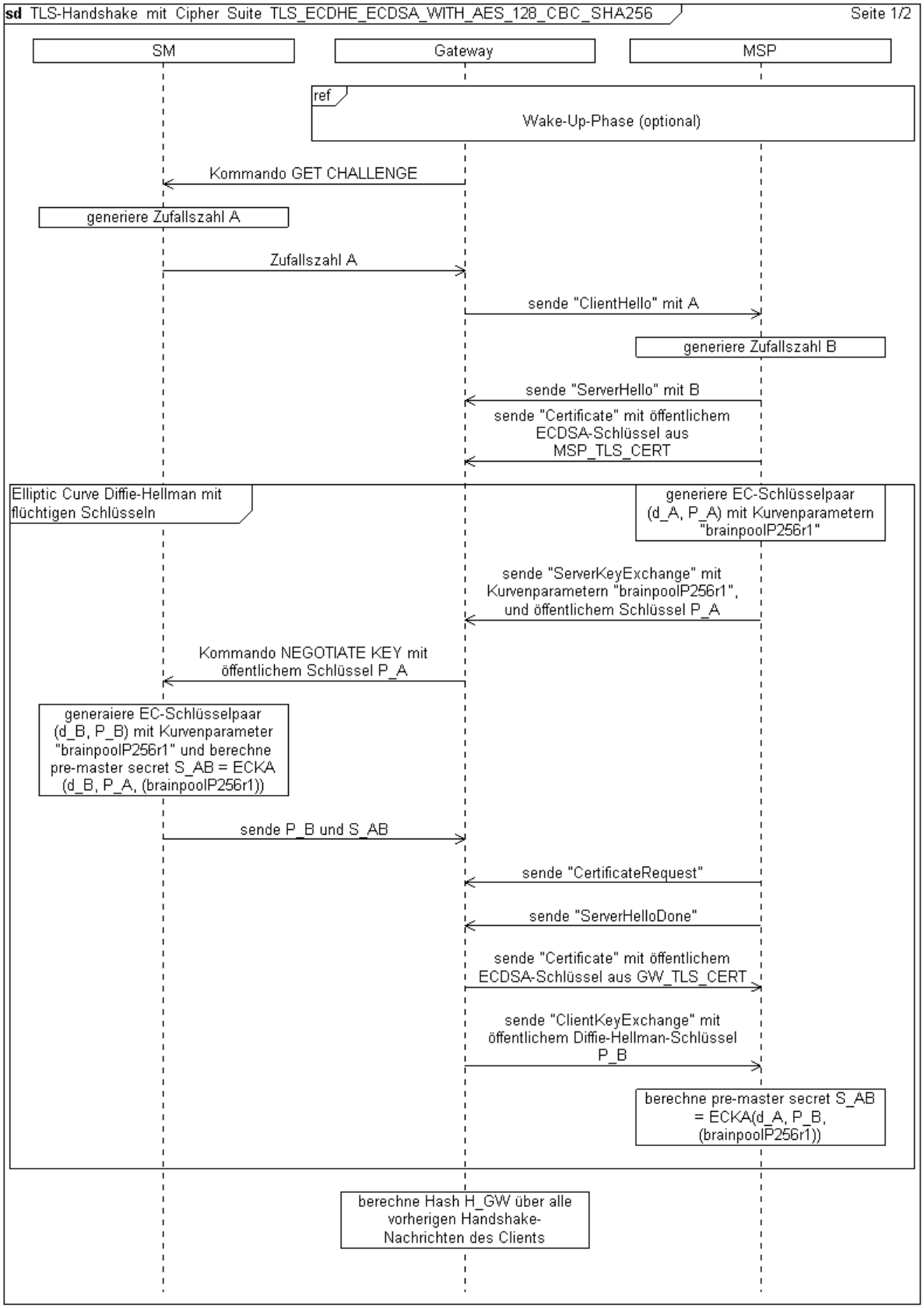


Abbildung 5: Sequenzdiagramm für die Interaktion zwischen Gateway und Sicherheitsmodul beim TLS-Handshake 1/2

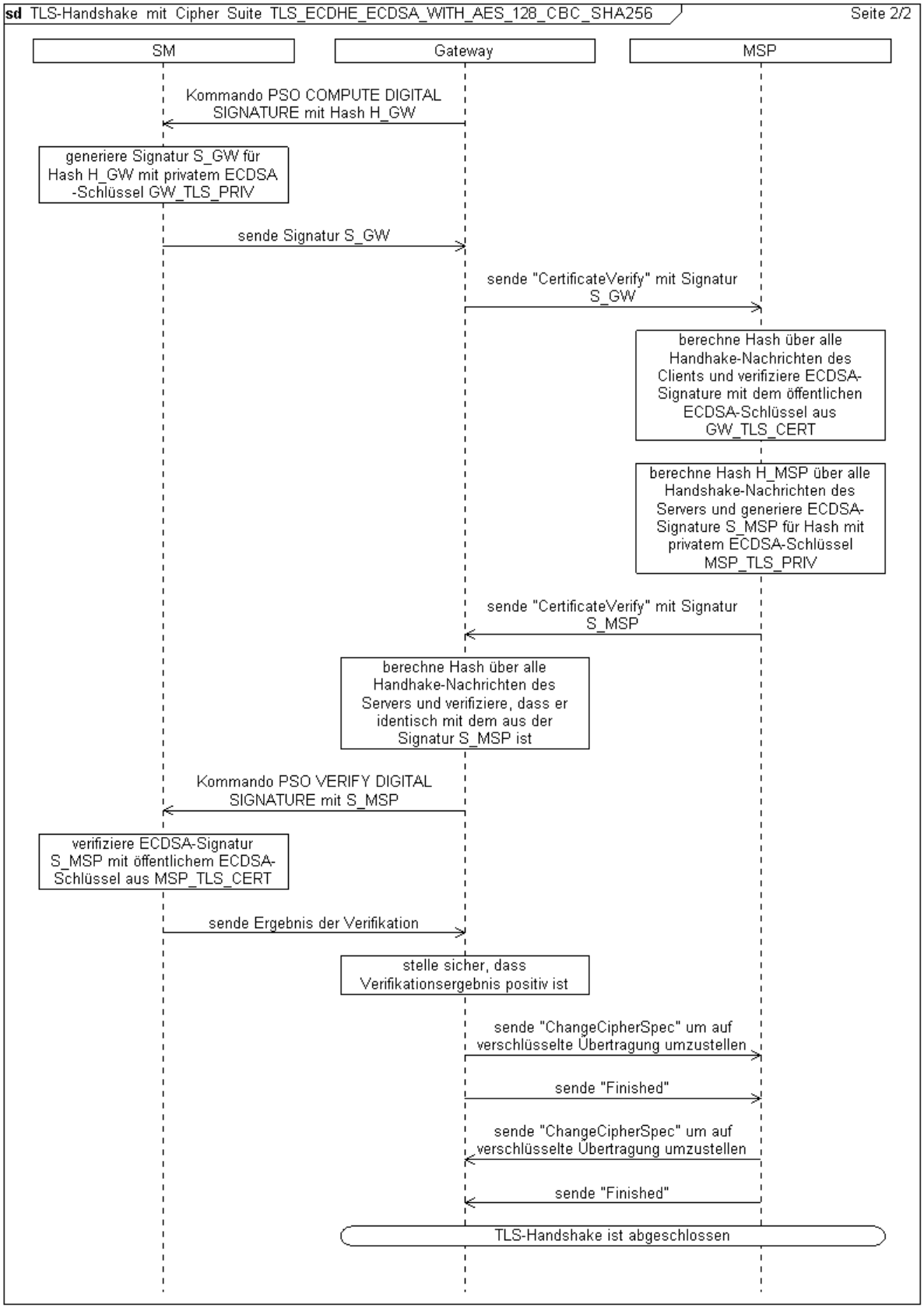


Abbildung 6: Sequenzdiagramm für die Interaktion zwischen Gateway und Sicherheitsmodul beim TLS-Handshake 2/2

Hinweis zu Abbildung 5 und Abbildung 6: Für den Aufbau von TLS-Kanälen zu anderen WAN-Teilnehmern, **MUSS** statt dem Zertifikat MSP_TLS_CERT das TLS-Zertifikat des jeweiligen WAN-Teilnehmers verwendet werden.

Die Reihenfolge der TLS-Kommandos beim TLS-Handshake **KANN** von der in den Abbildungen gezeigten Reihenfolge eventuell abweichen. Die Abbildungen sind diesbezüglich lediglich exemplarisch zu verstehen. Ausschlaggebend ist der TLS-Standard [TLS], aus dem sich Abhängigkeiten bezüglich der Reihenfolge der spezifizierten Kommandos ergeben. Alle genannten Kommandos sind verpflichtend.

3.2.2.2 Verschlüsselung, Integritätssicherung und Signierung auf Inhaltsdatenebene

Das Gateway **MUSS** mit Hilfe des Sicherheitsmoduls Inhaltsdaten (Netzstatusdaten, Abrechnungsdaten) mit einem symmetrischen Verschlüsselungsverfahren verschlüsseln.

Weiterhin **MUSS** das Gateway die verschlüsselten Inhaltsdaten mit einem MAC sichern.

Die verschlüsselten Inhaltsdaten **MÜSSEN** weiterhin mit einer kryptographischen Signatur gesichert werden.

Die Schlüssel für Inhaltsdatenverschlüsselung und MAC-Sicherung **MÜSSEN** durch einen auf elliptischer Kurven basierenden Schlüsselaustausch hergeleitet werden. Hierbei **MUSS** zudem eine entsprechende Schlüsselableitungsfunktion (KDF) verwendet werden. Das Gateway **MUSS** hierzu die Vorgaben aus Anhang A umsetzen.

Die Hash-Generierung, die symmetrische Verschlüsselung sowie die Schlüsselableitung **MÜSSEN** vom Gateway implementiert werden. Schlüsselaushandlung (NEGOTIATE KEY) und Signaturgenierung (PSO COMPUTE DIGITAL SIGNATURE) **MÜSSEN** vom Sicherheitsmodul umgesetzt werden. Anhang A zeigt hierzu die zu verwendenden kryptographischen Algorithmen und Schlüssellängen auf.

Die folgende Abbildung zeigt die Interaktion zwischen Gateway und Sicherheitsmodul im Bereich der Inhaltsdatenverschlüsselung, Integritätssicherung und Signierung.

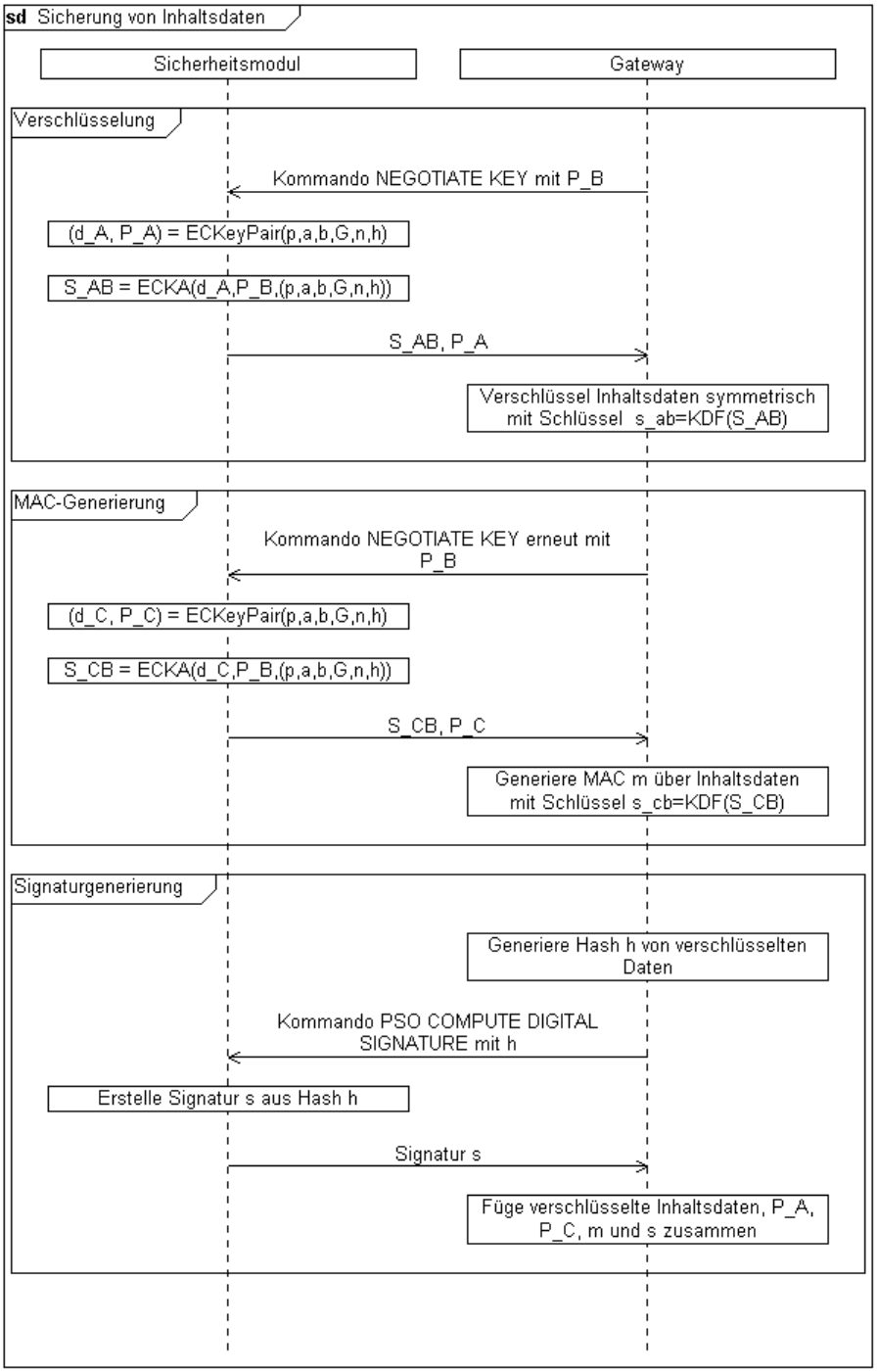


Abbildung 7: Sequenzdiagramm für die Interaktion zwischen Gateway und Sicherheitsmodul bei der Inhaltsdatensicherung

Der öffentliche Schlüssel P_B mit dem dazugehörigen privaten Schlüssel p_B ist im Besitz des Empfängers auf der WAN-Seite.

Die verschlüsselten Inhaltsdaten, die öffentlichen Schlüssel P_A und P_C, der MAC und die Signatur werden entsprechend den folgenden Kapiteln 3.2.3 und 3.2.4 in eine SOAP-Nachricht verpackt.

3.2.3 Kommunikationsprotokolle für Messdaten

3.2.4 Kommunikationsprotokoll für Administration

3.2.5 Wake-Up-Service

Dieser Abschnitt beschreibt den Wake-Up-Service, der von einem Smart Metering Gateway umzusetzen ist.

3.2.5.1 Allgemeine Beschreibung

TLS-Verbindungen, die zwischen Gateway und Teilnehmern im WAN verwendet werden, **MÜSSEN** immer vom Gateway als TLS-Client initiiert werden. Über einen sogenannten Wake-Up-Service **MUSS** es jedoch möglich sein, dass der Gateway Administrator über ein einfaches Datenpaket den Aufbau des TLS-Kanals anfordern kann.

Das Wake-Up-Paket (siehe Abschnitt 3.2.5.2) **MUSS** eine Geräteidentifizierung des adressierten Smart Meter Gateways und einen Zeitstempel enthalten. Diese Felder **MÜSSEN** mit dem privaten Schlüssel des Gateway-Administrators für die Inhaltsdatensignierung signiert werden. Die Informationen im Wake-Up-Paket sind nicht vertraulich und **werden** daher **nicht** verschlüsselt.

3.2.5.2 Datenstruktur des Wake-Up-Pakets

Das unsignierte Wake-Up-Paket **MUSS** folgenden Aufbau haben:

Header		Ver	RecipientId (9 Bytes)									Timestamp (8 Bytes)			
W	U	01h	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh
Timestamp (Forts.)			Padding / Reserved (12 Bytes)												
xxh	xxh	xxh	xxh	00h	00h	00h	00h	00h	00h	00h	00h	00h	00h	00h	00h

Tabelle 1: Aufbau des Wake-Up Paketes

Feld	#Bytes	Beschreibung
Header	2	Header = „WU“ (ASCII “57h 55h” = “0101.0111.0101.0101b”)
VersionId	1	Wake-Up-Paket Version = 01h
RecipientId	9	Ein-eindeutige Geräte-Identifikation des Empfänger Gateways. Kodierung für die Adressierungs-Variante gemäß Normentwurf E DIN 43863-5:2010-07 Byte[1] - Sparte (01h..0Fh) Byte[2-4] - Hersteller Identifikation (3 ASCII Buchstaben) Byte[5] - Fabrikationsblock (00h..FEh) Byte[6-9] - Fabriknummer (max. Dezimal 99.999.999)
Timestamp	8	UTC UnixTime als 64 Bit Signed Integer (Anzahl Sekunden seit dem 1. Januar 1970 00:00h UTC).
Padding / Reserved	12	Mit Nullen gefüllter Anhang, damit der Datensatz 32 (2*16) Bytes lang wird. Ggfs. für zukünftige Erweiterungen.

Tabelle 2: Felder im Wake-Up Paket

Das Wake-Up-Paket beginnt mit einem Zwei-Byte-Header „WU“, gefolgt von einem Byte VersionId, 9 Bytes für die RecipientId, 8 Bytes für den Timestamp und 12 Bytes Padding.

Das Feld ***Header*** dient zur Kennzeichnung des Wake-Up-Pakets und ermöglicht eine erste einfache (hardwarenahe) Überprüfung bzw. Klassifizierung der empfangen Pakete.

Das Feld ***VersionId*** bezeichnet die verwendete Version der Wake-Up-Paket Definition. Bei eventuellen zukünftigen Erweiterungen werden neue Versionsnummern vergeben.

Das Feld ***RecipientId*** dient zur eindeutigen Identifizierung des Empfänger Gateways. Nur das adressierte Smart Meter Gateway darf das Wake-Up-Paket verarbeiten. Hiermit soll verhindert werden, dass das Wake-Up-Paket von einem Angreifer missbraucht wird, um eine Vielzahl von Gateways in der Verantwortung eines Gateway-Administrators zu einem gleichzeitigen TLS Call-Back zu verleiten (DoS-Attacke).

Das Feld ***Timestamp*** enthält die aktuelle Zeit (in UTC) zum Zeitpunkt der Erstellung des Wake-Up-Pakets. Geringfügige Unterschiede zwischen den jeweiligen Uhrzeiten auf den Servern und den Gateways sind üblich. Der Timestamp muss daher in ein festgelegtes Zeitfenster relativ zur Uhrzeit des Smart Meter Gateways liegen (5 Sekunden).

Der Timestamp dient dazu, dass ein einzelnes Wake-Up-Paket nicht mehrfach für den Aufbau von TLS-Kanälen wiederverwendet werden kann (Replay-Attacke).

Dem Feld Timestamp folgen 12 ***Padding*** Nullbytes, um den Datensatz auf 32 (2*16) Bytes aufzufüllen. Diese können gegebenenfalls für zukünftige Erweiterungen verwendet werden.

Anschließend wird vom Gateway-Administrator ein SHA256-Hash über die 32 Bytes generiert. Der Hash wird mit ECDSA und einer elliptischen Kurve gemäß Anhang A signiert (siehe [TR-03111, 4.2.1). Die Signatur (*r, s*) wird im "Plain Format" kodiert, das heißt die Werte *r* und *s* werden einfach an das Wake-Up-Paket angehängt.

Header		Ver	RecipientId (9 Bytes)									Timestamp (8 Bytes)			
W	U	01h	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh
Timestamp (Forts.)			Padding / Reserved												
xxh	xxh	xxh	xxh	00h	00h	00h	00h	00h	00h	00h	00h	00h	00h	00h	00h
ECDSA-Signature (r) (32 Bytes)															
xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh
xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh
ECDSA-Signature (s) (32 Bytes)															
xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh
xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh	xxh

Tabelle 3: Signiertes Wake-Up Paket

Die in Tabelle 3: Signiertes Wake-Up PaketTabelle 3 abgebildete Struktur mit der Länge von 96 Bytes wird als Wake-Up-Paket an das Gateway versendet.

3.2.5.3 Anforderungen an den Transportweg des Wake-Up-Pakets

Es existieren keine Anforderungen an den Transportweg des Wake-Up-Pakets. Das Paket wird über eine im Gateway verbaute WAN-Schnittstelle empfangen. Diese Schnittstelle ist nicht zwingenderweise identisch mit der WAN-Schnittstelle über die anschließend auch der TLS-Kanal aufgebaut wird.

3.2.5.4 Verarbeitung eines Wake-Up-Pakets

Die folgenden Verarbeitungsregeln gelten für das Gateway:

1. Bei Empfang eines (potentiellen) Wake-Up-Pakets **MUSS** (in dieser Reihenfolge) geprüft werden ob,
   a. die Kennzeichnung des Wake-Up-Pakets übereinstimmt.
      Damit das Gateway nicht bei jedem empfangenem Paket eine vollständige Wake-Up-Paket Prüfung vornimmt, sind zuerst die ersten drei Bytes des Pakets (Header+Version) zu überprüfen. Diese MÜSSEN der Zeichenkette „WU“ und der aktuelle Version (01h) entsprechen.
   b. das Smart Meter Gateway Adressat dieses Paketes ist.
      Dazu wird die im Paket enthaltene Geräteidentifizierung mit den Identifikationsdaten

des Smart Meter Gateways verglichen. Die beiden Werte **MÜSSEN** übereinstimmen.

c. die Nachricht in einem akzeptablen Zeitrahmen versendet/empfangen worden ist. Dazu ist im Wake-Up-Paket einen Zeitstempel enthalten. Der übertragene Zeitstempel **DARF NICHT** älter als 5 Sekunden verglichen mit der aktuellen Systemzeit im Gateway sein. Dies soll das Wiederverwenden des Paketes zu einem beliebigen Zeitpunkt verhindern.

d. die Signatur des Pakets vom Gateway-Administrator stammt.
Die Dienste des Sicherheitsmoduls werden dabei für die Signaturprüfung verwendet. Um DoS-Attacken des Gateways zu erschweren **MUSS** das Gateway die Anzahl der Wake-Up-Paket Signaturprüfungen innerhalb eines Zeitraumes einschränken.

2. Konnten Teile der Inhalt der Nachricht nicht verifiziert werden, d.h. die Überprüfung der Kennzeichnung, der Geräteidentifizierung, des Zeitstempels oder der Signatur sind fehlerhaft, so wird der weitere Prüfungsvorgang beim ersten Fehler unterbrochen und die Nachricht sofort verworfen. Es **DARF KEIN** Feedback zum Teilnehmer im WAN zurückgesendet werden. Der entsprechende Prozess terminiert.
3. Konnte der Inhalt der Nachricht verifiziert werden, so wird die Nachricht auch jetzt verworfen. Es **DARF KEIN** Feedback zum Sender zurückgeschickt werden. Vom Gateway **MUSS** jedoch ein TLS-Kanal zu dem vorkonfigurierten externen Teilnehmer im WAN initiiert werden, sofern dieser TLS-Kanal nicht schon aufgebaut ist. Der entsprechende Teilnehmer **MUSS** im Gateway vorkonfiguriert sein.

3.2.6 Zeitdienst

- Kommunikationsablauf/ Synchronisation GW □□ Gateway Administrator

3.3 Vorgaben an die Kommunikationsverbindungen in das LMN

3.3.1 Übersicht

Dieses Kapitel hat informativen Charakter.

Im LMN kommuniziert das Gateway mit einem oder mehreren Zählern, um von diesen Messwerte zu erhalten.

Anwendungsprotokolle für die Übermittlung von Messwerten werden in Kapitel 3.3.3 beschrieben.

Abhängig davon, ob ein Zähler in das Gehäuse des Gateways integriert wird, muss eine Sicherung der Kommunikation stattfinden, die in Kapitel 3.3.2 in zwei Ausprägungen beschrieben wird. Abbildung 9 zeigt die Einordnungen dieser beiden Kommunikationsmodelle im Vergleich zum ISO-Referenzmodell und dem TCP/IP-Modell.

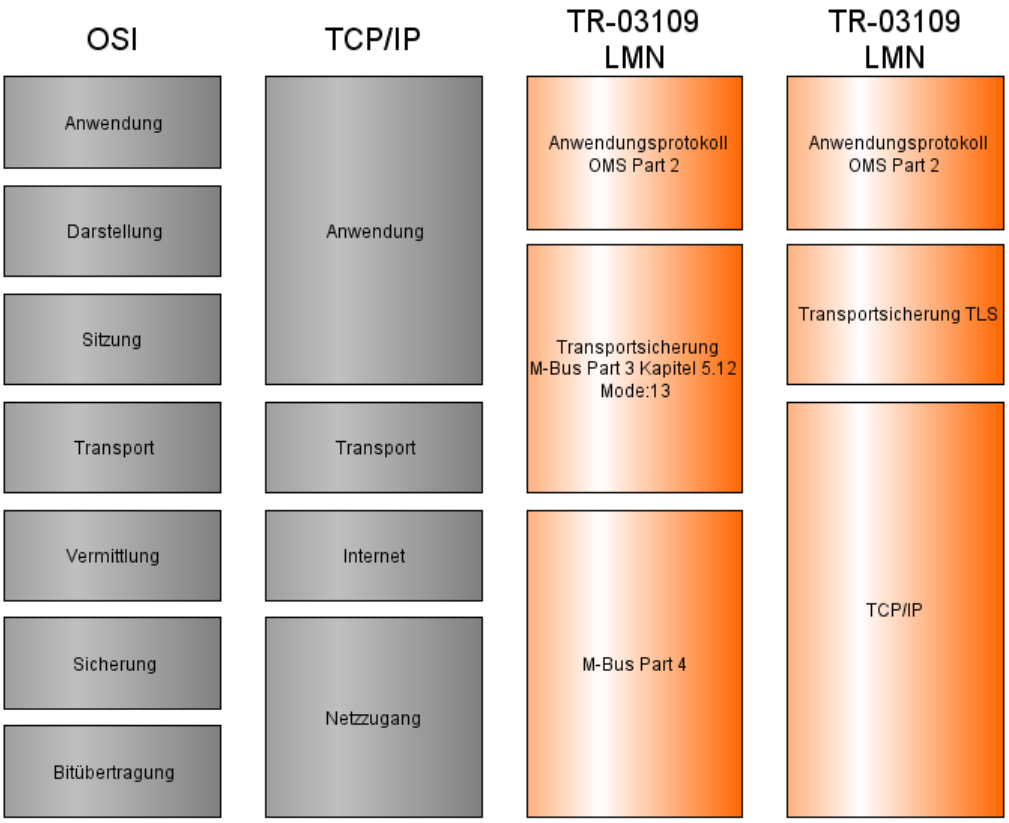


Abbildung 8: Kommunikationsmodelle im LMN

3.3.2 Sicherung der Kommunikationsverbindungen in das LMN

Das Gateway **MUSS** sicherstellen, dass Messwerte, die von Zählern empfangen werden, nur dann akzeptiert werden, wenn sie über eine gesicherte Kommunikation vor Abhören, Manipulation und Fälschung geschützt werden. Das Gateway **MUSS** dabei Sicherungen für uni- und bidirektionale Kommunikation unterstützen, wie in den folgenden Unterkapiteln dargestellt.

Das Gateway **DARF** zudem Messwerte von Zählern akzeptieren, die über ungesicherte Kommunikation empfangen werden, sofern die physikalische Umgebung des Gateways dies zulässt. Anforderungen bezüglich der physikalischen Umgebung sind Kapitel 6 zu entnehmen.

3.3.2.1 Bidirektionale Kommunikation (TLS)

Das Gateway **MUSS** TLS implementieren, damit Zähler, die für eine bidirektionale Kommunikation ausgelegt sind, verwendet werden können.

Die Anforderungen an die TLS-Kommunikation mit den Zählern entsprechen den Anforderungen aus Kapitel 3.2.2.1, wobei die Rolle des WAN-Teilnehmers nun durch die Rolle des Zählers ersetzt wird. Das Gateway **MUSS** diese Anforderungen auch für die Zählerkommunikation erfüllen.

Zusätzlich zu dem in Kapitel 3.2.2.1 dargestellten Ablauf, **MUSS** das Gateway auch die Rolle des TLS-Servers übernehmen können. In diesem Fall baut der Zähler als TLS-Client die Verbindung zum Gateway auf. Auch als TLS-Server **MUSS** das Gateway sein Sicherheitsmodul für die in Kapitel 3.2.2.1.2 dargestellten kryptographischen Operationen verwenden.

Das Anwendungsprotokoll für die Zählerkommunikation (s. Kapitel 3.3.3) setzt im Fall der bidirektionalen Kommunikation direkt auf den TLS-Kanal auf.

3.3.2.2 Unidirektionale Kommunikation

3.3.2.2.1 Protokollübersicht

Dieses Kapitel hat informativen Charakter.

Bei der unidirektionalen Kommunikation ist der Zähler der Sender von Nachrichten und das Gateway der Empfänger. Das in Kapitel 3.3.3 definierte Anwendungsprotokoll wird daher über symmetrische Kryptographie gesichert (siehe Anhang A).

Kapitel 3.3.3 legt fest, welche Bereiche des Anwendungsprotokolls durch dieses Verfahren entsprechen zu sichern sind.

Das folgende Unterkapitel spezifiziert nun die Anforderungen, die für diese Art der Sicherung vom Gateway umgesetzt werden müssen.

3.3.2.2.2 Anforderungen an die Sicherung der unidirektionalen Kommunikation

Das Gateway **MUSS** die kryptographischen Algorithmen implementieren, die für die symmetrische Zählerdatensicherung in Anhang A gefordert sind. Entsprechende Funktionalitäten zum Einbringen des Master-Keys in das Gateway im Rahmen der Konfiguration eines Zählers werden in Kapitel 5.3 behandelt.

Das Gateway **MUSS** bei Empfang eines Datensatzes den MAC mit dem zuvor abgeleiteten Schlüssel K_{MAC} prüfen. Es **DARF** den verschlüsselten Datensatz **NICHT** auswerten oder anderweitig verwenden, wenn der MAC nicht verifiziert werden konnte.

Weiterhin **MUSS** das Gateway den Wert von Z betrachten. Es **DARF** den verschlüsselten Datensatz **NICHT** auswerten oder anderweitig verwenden, wenn dieser Wert kleiner oder gleich dem zuletzt erhaltenen Wert für Z ist. Das Gateway **MUSS** sich deshalb für jeden angeschlossenen Zähler den Wert von Z nach jeder erfolgreichen Übermittlung merken. Der Mechanismus verhindert, dass mitgeschnittene Zählerdaten von einem Angreifer wiederholt an das Gateway übermittelt werden können (Replay-Attacke).

Ist der MAC korrekt, so **MUSS** das Gateway den verschlüsselten Datensatz mit dem Schlüssel K_{ENC} entschlüsseln. Der entschlüsselte Datensatz **MUSS** dann entsprechend Kapitel 3.3.3 behandelt werden.

3.3.3 Kommunikationsprotokolle

In diesem Abschnitt werden die Anforderungen an das Smart Meter Gateway in Bezug auf die zu unterstützenden Kommunikationsprotokolle im LMN festgelegt. Prinzipiell wird hier unterschieden zwischen Anforderungen, die auf die Unterstützung von Applikationsdatenformaten abzielen, und Anforderungen an das Schnittstellenprotokoll für den Transport der Applikationsdaten.

Das Format der Daten und die Protokolle der internen Kommunikationsverbindungen bei einer One-Box-Solution werden nicht vorgeschrieben. Es wird aber empfohlen auch hier die in diesem Kapitel aufgestellten Interoperabilitätsanforderungen einzuhalten.

Darüber hinaus **MÜSSEN** bei einer One-Box-Solution externe Schnittstellen für den Anschluss von weiteren, nicht eingebauten Mess-Einrichtungen im LMN bereitgestellt werden. Werden diese Schnittstellen nicht genutzt, **MÜSSEN** sie durch den Gateway-Administrator deaktiviert werden können.

3.3.3.1 Applikationsprotokolle

Die Struktur der Messdaten (die Anwendungsdaten) bei der Kommunikation zwischen Zähler und Gateway **MUSS** den Vorgaben der OMS Spezifikation Volume 2 [OMS-2] Kapitel 4 „Application Layer“ genügen. OMS fordert die Unterstützung folgender Anwendungsprotokolle:

- M-Bus DIN EN 13757-3: Kommunikationssysteme für Zähler und deren Fernablesung Teil 3: Spezieller Application Layer
- DLMS/COSEM: DIN EN 62056-61 Object Identification System (OBIS), DIN EN 62056-62 Interface-Klassen, DIN EN 62056-53 COSEM-Anwendungsschicht
- SML Smart Message Language: prEN 62056-5-8

Dies bedeutet, dass das Smart Meter Gateway die Datenstrukturen dieser Applikationsprotokolle mindestens insoweit implementieren **MUSS**, dass es die empfangenen und zur weiteren Bearbeitung notwendigen Messwerte extrahieren und verarbeiten kann.

Die Unterstützung weiterer Anwendungsprotokolle mit den zugehörigen Datenformaten (z.B. IEC 61850, CIM IEC 61968/61970, ZigBee SEP2, KNX, OASIS Energy Interoperation, ANSI C12.22, FNN-SyM^2, usw.) ist erlaubt. Allerdings **MUSS** die Übertragung der Daten über einen sicheren Transportkanal, wie in Kapitel 3.3.2 beschrieben, erfolgen.

Eine Verschlüsselung oder Signierung der **Inhaltsdaten** durch den Zähler wird nicht gefordert.

3.3.3.2 Übertragungsprotokolle

Drahtlose Schnittstelle

Das Smart Meter Gateway **MUSS** eine Funkschnittstelle zum drahtlosen Anschluss von Messeinrichtungen besitzen. Das auf der Funkschnittstelle realisierte Übertragungsprotokoll **MUSS** kon-

744 form sein zur Norm [-4] „M-Bus DIN EN 13757-4, Kommunikationssysteme für Zähler und deren
745 Fernablesung Teil 4: Zählerauslesung über Funk, Fernablesung von Zählern im SRD-Band von 868
746 MHz bis 870 MHz" - im Folgenden kurz wM-Bus genannt.

747 Gemäß der OMS Spezifikation [OMS-1] **MUSS** das Smart Meter Gateway alle Zähler unterstützen,
748 die in folgenden Betriebsarten arbeiten.

Betriebsart	Kommunikation	m/o[1]	Beschreibung
S1	unidirektional	m	Zähler überträgt einige Male je Tag zu einem ortsfesten Empfangspunkt
S2	bidirektional	m	Zählereinheit mit einem Empfänger, der ständig bereit ist oder synchronisiert arbeitet, ohne erweiterte Vorbereitung für das Wecken
T1	unidirektional	m	Übertragung nur in kurzen Datenblöcken in kurzen Zeitabständen
T2	bidirektional	m	Die Zählereinheit übermittelt regelmäßig wie Betriebsart T1, und deren Empfänger wird nach dem Ende jeder Übertragung für eine kurze Dauer eingeschaltet und rastet ein, wenn er eine Rückmeldung erhält
R2	bidirektional	o	Zähler ist regelmäßig empfangsbereit und kann geweckt werden. Danach ist ein Dialog mit dem Transceiver möglich

749 *Tabelle 4: Betriebsarten für wM-Bus*

750 Die Sicherung der Kommunikation in den Modi S1 und T1 (unidirektional) **MUSS** mittels der in
751 Kapitel 3.3.2.2 beschriebenen symmetrischen Kryptographie geschehen. Die Sicherung der Kom-
752 munikation in den bidirektionalen Modi S2, T2 und R2 **MUSS** mittels TLS implementiert sein (sie-
753 he Kapitel 3.3.2.1).

754 **Drahtgebundene Schnittstelle**

755 Das Smart Meter Gateway **MUSS** eine Schnittstelle zum drahtgebundenen Anschluss von Messein-
756 richtungen besitzen. Diese Schnittstelle **MUSS** als Ethernet-Schnittstelle mit Unterstützung von
757 TCP/IP realisiert werden. Diese Schnittstelle kann dem Anschluss von Stromzählern dienen oder
758 anderer Zähler, die z.B. mittels eines Zähler-Adapters proprietäre Übertragungsprotokolle auf E-
759 thernet mit TCP/IP transformieren.

760 Weitere drahtgebundene Schnittstellen (z.B. Lo-Bus DIN EN 13757-6, M-Bus drahtgebunden DIN
761 EN 13757-2, RS485, …) sind erlaubt und können im Smart Meter Gateway bereitgestellt werden.
762 Oberhalb dieser drahtgebundenen Übertragungsprotokolle **MUSS** für bidirektionale Kommunikati-
763 on TLS gemäß Kapitel 3.3.2.1 und für unidirektionale Kommunikation die in Kapitel 3.3.2.2 be-
764 schriebene symmetrische Kryptographie als Transportsicherung eingesetzt werden.

[1] m = muss, o = optional

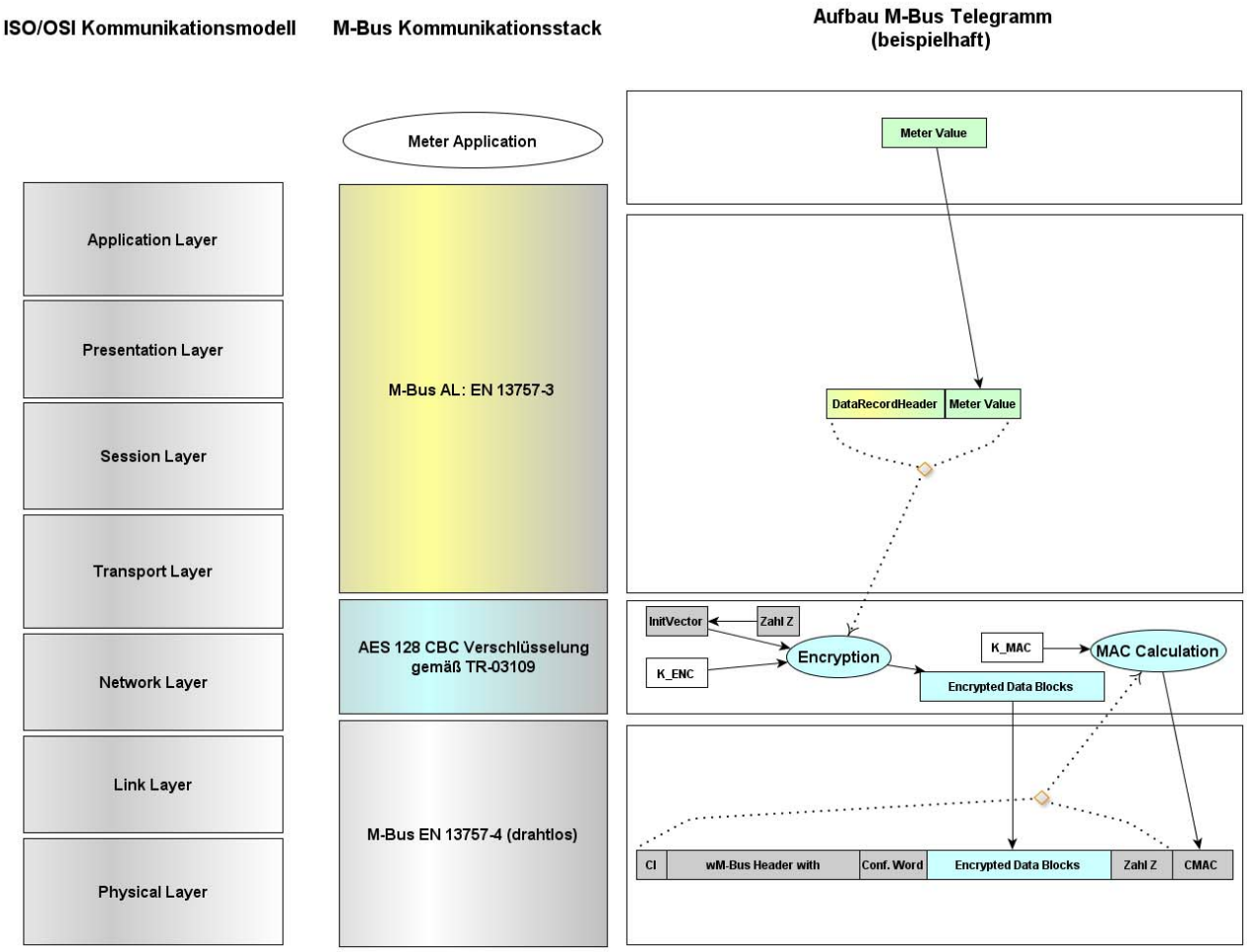
765 ### 3.3.3.3 Beispiel: Anschluss wM-Bus Zähler (unidirektionale Kommunikation)

766 Die folgende Abbildung zeigt den Protokollstack im Smart Meter Gateway für die Anbindung eines
767 wM-Bus Zählers, der seine Daten im M-Bus Application Layer Format sendet. Die in M-Bus trans-
768 portierten Anwendungsdaten müssen mittels AES CBC gemäß Anhang A verschlüsselt werden.

769 Die Sicherung der Integrität der gesendeten Daten erfolgt durch die Anwendung des MAC-
770 Algorithmus auf das gesamte wM-Bus Telegramm, d.h.

771 • beginnend mit dem CI-Byte (Control Information Byte) über alle wM-Bus Header Daten
772 • über den verschlüsselte Datensatz
773 • bis hin zum und einschließlich des Pre-Initialisierungsvektors (d.h. des Zählers), der unver-
774 schlüsselt an die verschlüsselten Datenblöcke angehängt wird

775 Der 16 Byte große CMAC **MUSS** unverschlüsselt an das Ende des wM-Bus Telegramm angehängt
776 werden.



777

778 *Abbildung 9: Wireless M-Bus Protokollstack*

3.3.3.4 Beispiel: Anschluss Stromzähler über TCP/IP

Die folgende Abbildung skizziert den Protokollstack im Smart Meter Gateway für die Anbindung eines Stromzählers, der seine Daten über TCP/IP im DLMS/COSEM Format sendet. Die Transportverbindung **MUSS** mittels TLS gesichert sein:

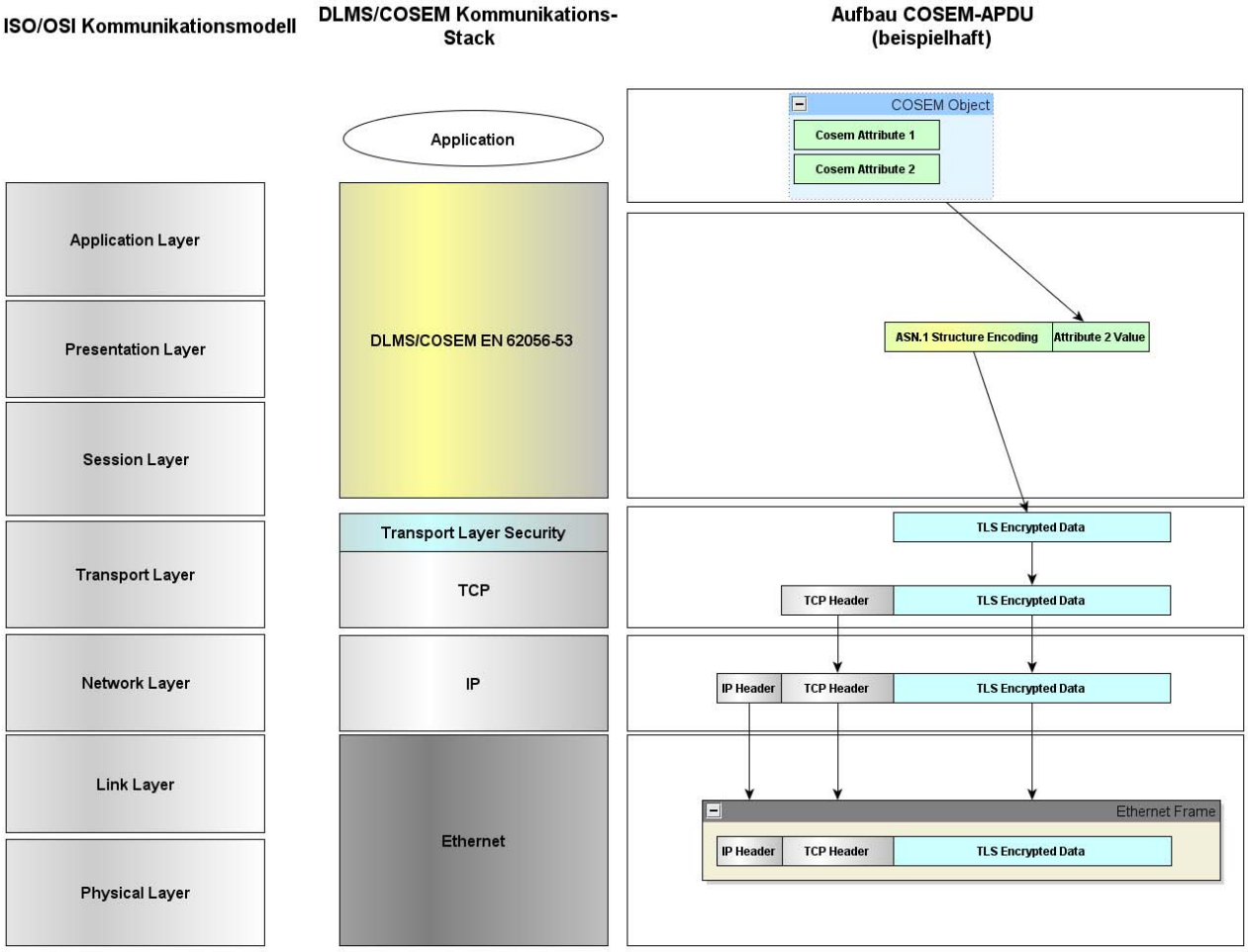


Abbildung 10: TCP/IP TLS Protokollstack

Der Wert von „Attribut 2“ eines COSEM Objektes wird mittels ASN.1 Encoding sequentialisiert und über einer durch TLS gesicherten TCP/IP Verbindung transportiert.

3.4 Vorgaben an die Kommunikationsverbindungen in das HAN

3.4.1 Übersicht

Dieses Kapitel hat informativen Charakter.

Dieses Kapitel behandelt die Anforderungen an das Gateway bezüglich der Kommunikation im HAN.

Das Gateway kommuniziert im HAN mit einer Anzeigeeinheit, um dem Verbraucher Einsicht in seine Verbrauchsdaten zu gewähren. Anforderungen dazu sind in Kapitel 3.4.2 spezifiziert.

Zudem dürfen CLS-Systeme im HAN vorhanden sein, die untereinander oder über einen Proxy-Dienst des Gateways mit WAN-Teilnehmern kommunizieren können. Kapitel 3.4.3 spezifiziert entsprechende Anforderungen.

3.4.2 Kommunikation mit der Anzeigeeinheit

3.4.2.1 Anzeige von Verbrauchswerten

Dieses Kapitel hat informativen Charakter.

Verbraucher haben den Bedarf, ihre eigenen Verbrauchswerte am Gateway zu überprüfen. Hierzu muss das Gateway eine Möglichkeit bereitstellen, diese Werte anzuzeigen. Dies kann entweder über eine im Gateway integrierte Anzeigeeinheit geschehen oder aber über eine abgesetzte Anzeigeeinheit im HAN.

Abgesetzte Anzeigeeinheiten können dedizierte Geräte für das Smart Metering-Umfeld sein oder aber weitere Geräte, wie etwa ein PC des Verbrauchers.

Für Anzeigeeinheiten werden Anforderungen an die Aufbereitung der Daten (HTML-Seiten, schema-konforme XML-Daten) gestellt. Weiterhin wird sich der Verbraucher für die Anzeige der Daten authentifizieren müssen. Das Anwendungsprotokoll in Kapitel 3.4.2.3 greift dies auf.

Kommunikation mit abgesetzten Anzeigeeinheiten findet über das Protokoll HTTPS (s. [RFC2818]) statt, in dem für die Absicherung der Kommunikation TLS verwendet wird (s. Kapitel 3.4.2.2).

Die physikalische Übertragung der Daten bis hin zu Transportschicht (nach OSI-Referenzmodell Schichten 1-4 [ISO7498-1]) werden in dieser TR nicht vorgegeben und können herstellerspezifisch sein. Auf Ihnen setzen das Protokoll zur Absicherung der Kommunikation auf.

3.4.2.2 Sicherung der Kommunikation

Das Gateway **MUSS** einen HTTPS-Server (HTTP über TLS) für abgesetzte Anzeigeeinheiten anbieten.

Das Gateway **MUSS** die beidseitige Authentifizierung mit TLS-Zertifikaten durchsetzen. Die zu verwendenden Zertifikate sind im Anhang C definiert.

Die Anforderungen an die TLS-Implementierung entsprechen den Anforderungen aus Anhang A. Zu beachten ist, dass die Anzeigeeinheit hier den Client darstellt und das Gateway den Server. Die Ciphersuite wird eventuell nicht von allen Browsern (z.B. Firefox und Chrome) unterstützt.

3.4.2.3 Kommunikationsprotokolle

HINWEIS: befindet sich in Arbeit.

- XML-Schema (nicht eichrechtlich relevant)
- https-Webseite, pures, statisches HTML (eichrechtlich relevant)
- Benutzerauthentifizierung

3.4.3 Sicherung der CLS-Kommunikation

3.4.3.1 Übersicht

Dieses Kapitel hat informativen Charakter.

CLS-Systemen im HAN soll es ermöglicht werden, über das Gateway mit konfigurierten Teilnehmern im WAN zu kommunizieren. Das Gateway stellt dafür eine Proxy-Funktionalität bereit. Es werden Anforderungen an die Sicherung der Kommunikation zur WAN-Seite gestellt und an die Sicherung der Kommunikation zwischen CLS und Gateway, für den Fall, dass das CLS nicht physisch im Gehäuse des Gateways integriert ist.

An die CLS-Daten oder an die zugrundeliegenden Anwendungsprotokolle werden in dieser Technischen Richtlinie keine Vorgaben gemacht.

3.4.3.2 Sicherung der Kommunikation

Das Gateway **MUSS** Kommunikation zwischen CLS-Systemen im HAN und konfigurierten WAN-Teilnehmern ermöglichen (s. Abbildung 11).

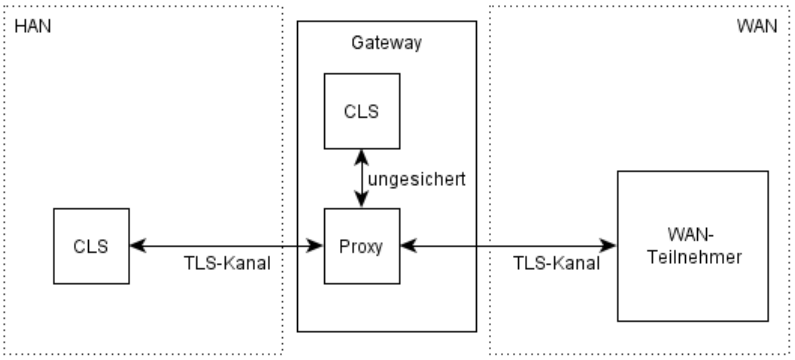


Abbildung 11: Absicherung der Kommunikation für CLS-Proxy

Die Kommunikation auf der Seite des WAN **MUSS** zwischen Gateway und WAN-Teilnehmer über eine beidseitig authentifizierte TLS-Verbindung gemäß Kapitel 3.2.2.1 abgesichert sein, in der das Gateway als TLS-Client auftritt und sein Sicherheitsmodul für die asymmetrischen kryptographischen Operationen verwendet.

847 Die Kommunikation auf der Seite des HAN **MUSS** zwischen CLS-System und dem Gateway ent-
848 weder über TLS gesichert sein oder aber das CLS-System **MUSS** durch die physikalische Umge-
849 bung[2] (z.B. Integration in das Gateway) geschützt sein. Im ersten Fall **MUSS** das Gateway TLS
850 gemäß Kapitel 3.2.2.1 implementieren und sowohl als TLS-Client als auch als TLS-Server agieren
851 können. Die Rolle des WAN-Teilnehmers ist dann durch die Rolle des CLS-Systems zu ersetzen.

852 Das Gateway **MUSS** sicherzustellen, dass seine Funktionalität nicht durch CLS-Systeme kompro-
853 mittiert werden kann. Insbesondere **MUSS** das Gateway verfügbar bleiben, auch wenn CLS-
854 Systeme unabsichtlich oder absichtlich fehlerhaft funktionieren. Die Kommunikation von CLS-
855 Systemen **MUSS** von der restlichen Kommunikation geeignet separiert werden. Folgende Maß-
856 nahmen **MÜSSEN** dafür umgesetzt werden:

857 - Physikalische Trennung der Schnittstellen zum WAN, HAN und LMN

858 - Beschränkung der Rechenzeit für Betriebssystemprozesse, die für CLS-Funktionalität zu-
859 ständig sind, so dass die Verfügbarkeit der restlichen Funktionalität nicht eingeschränkt
860 werden kann.

[2] Spezifische Anforderungen an die physikalische Umgebung des Gateways sind im Kapitel 6 zu finden.

4 Tarifprofile und Tarifierung

4.1 Einleitung

Dieses Kapitel hat informativen Charakter.

4.2 Tarifierungsarten

4.3 Berechtigungsprofile

- Spezifikation des XML-Schematas
- Einbringung von Administrationskommandos in Profile
- Erweiterungsfreiheit für Hersteller

869 # 5 Weitere Funktionale Anforderungen

870 ## 5.1 Logdatenformat

871 Dieses Kapitel beinhaltet Vorgaben an die Syntax von Log-Informationen, die das Smart Meter
872 Gateway an den Schnittstellen (WAN, HAN) zur Verfügung stellen muss.

873 Das Smart Meter Gateway **MUSS** gemäß Schutzprofil [GW_PP] Kapitel 4.1, Sicherheitsziel O.Log
874 mindestens drei Klassen von Log-Informationen implementieren:

Log-Klasse	Zugriff	Schnittstelle
System-Log	lesender Zugriff durch den autorisierten Gateway Administrator	WAN Schnittelle
Kunden-Log	lesender Zugriff nur durch den authentifizierten und autorisierten Anschlussnutzer auf die ihm zugeordneten Log-Einträge	HAN Schnittstelle (Schnittstelle für die Anzeigeeinheit)
Eichtechnisches Log	lesender Zugriff durch den autorisierten Gateway Administrator	WAN Schnittelle

875 *Tabelle 5: Log-Klassen und erlaubter Zugriff*

876 Die konkrete Implementierung der Log-Informationen **KANN** so realisiert werden, dass tatsächlich
877 drei separate Dateien beschrieben werden. Andere Implementierungen (z.B. als Log-Records in
878 einer Datenbank) sind ebenfalls möglich. Die Zugriffsbeschränkungen auf diese Log-Records
879 **MÜSSEN** allerdings, wie in obiger Tabelle beschrieben, auf jeden Fall umgesetzt werden.

880 Die folgenden Informationen **MUSS** jeder Log-Eintrag beinhalten:

Merkmal	Bedeutung	o/m[3]
record_number	Eine eindeutige Zahl, die diesen Log-Eintrag kennzeichnet	m
datetime	Datum und Uhrzeit in UTC (Universal Coordinated Time), wann der Log-Eintrag geschrieben wurde, z.B. „2011-09-06T12:34:47“	m
level	Loglevel, die Einstufung der Wichtigkeit des Logeintrages • „I“: Info allgemeine Information zum normalen Ablauf • „W“: Warning Auftreten einer unerwarteten Situation • „E“: Error behebbarer Fehler oder Ausnahme, die Bearbeitung wurde alternativ fortgesetzt. • „F“: Fatal kritischer Fehler, die laufende Bearbeitung wurde abgebrochen.	m
event_type	Art des aufgezeichneten Events • Auftreten eines sicherheitsrelevanten Ereignisses	m

[3] o: optional, m: mandatory, d.h. verpflichtend

	• Verbindungsauf- bzw. abbau zu WAN Teilnehmer • Übertragung abrechnungsrelevanter Messdaten zu WAN Teilnehmer • Übertragung nicht abrechnungsrelevanter Messdaten zu WAN Teilnehmer • Erstellen/Löschen/Bearbeiten eines Berechtigungsprofils • Änderung der Gateway Konfiguration durch den Administrator • Änderung eines eichrechtlich gesicherten Parameters • Start und Stopp des Log-Mechanismus • weitere Events, die in den Security Requirements des Schutzprofils (bzw. in [CCPart2V3.1]) definiert sind	
subject_identity	Identität des Subjektes (Prozess, Anwendungskomponente, Benutzer, Profil), durch das ein Event ausgelöst wurde.	o
outcome	Ergebnis, der mit dem Log-Event verbundenen Aktionen • „S“: Success Die Aktion wurde erfolgreich abgeschlossen • „F“: Failure Die Aktion konnte nicht erfolgreich durchgeführt werden.	m
message	Eine das Log-Event zusätzlich beschreibende Erklärung bzw. die Parameter des geloggten Events. Diese sind abhängig vom „event_type“.	m
user_identity	Die Identität des Benutzers, durch den das Event ausgelöst wurde, bzw. für den die Aktion durchgeführt wurde. Bei der Übertragung von Messdaten an WAN Teilnehmer **MUSS** in diesem Feld insbesondere die Identität des Anschlussnutzers geloggt werden, dessen Daten übermittelt wurden. Die Log-Einträge im Kundenlog **MÜSSEN** das Attribut „user_identity“ gesetzt haben. Dadurch soll gewährleistet werden, dass verschiedene Anschlussnutzer nur die für sie bestimmten Kundenlog-Einträge in der Anzeigeeinheit dargestellt bekommen (Mandantenfähigkeit des Smart Meter Gateways).	o
destination	Adresse des Kommunikationspartners beim Verbindungsaufbau und Datenaustausch (z.B. URL)	o
evidence	Signatur der übertragenen Messdaten durch das Smart Meter Gateway, zur Beweisbarkeit der Authentizität und des Ursprungs der übertragenen Messdaten	o

Tabelle 6: Elemente eines Log Eintrages

Die Syntax der Log-Einträge für alle drei Log-Klassen beim Auslesen an der WAN bzw. HAN Schnittstelle durch den Gateway Administrator bzw. einen berechtigten Benutzer **MUSS** dem folgenden XML Schema genügen:

```
<?xml version="1.0" encoding="utf-8"?>
<!-- Document smgw_log.xsd: xml schema for smart meter gateway log information (system-, consumer-,
  calibration-log) -->
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:smgw="http://smgw.bsi.bund.de/schema/tr/smgw/1.0"
  xmlns:smgwlog="http://smgw.bsi.bund.de/schema/tr/smgw_log/1.0" targetNamespa-
ce="http://smgw.bsi.bund.de/schema/tr/smgw_log/1.0"
  elementFormDefault="qualified" attributeFormDefault="unqualified" version="1.0">

  <xs:simpleType name="type.loglevel">
    <xs:annotation>
      <xs:documentation>Short cut for log level: I(NFO), W(ARNING), E(RROR), F(ATAL)
      </xs:documentation>
    </xs:annotation>
    <xs:restriction base="xs:string">
      <xs:enumeration value="I" />
      <xs:enumeration value="W" />
      <xs:enumeration value="E" />
      <xs:enumeration value="F" />
    </xs:restriction>
  </xs:simpleType>

  <xs:simpleType name="type.outcome">
    <xs:annotation>
      <xs:documentation>Short cut for operational(S)uccess/(F)ailure
      </xs:documentation>
    </xs:annotation>
    <xs:restriction base="xs:string">
      <xs:enumeration value="S">
        <xs:annotation>
          <xs:documentation>Operation with success</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="F">
        <xs:annotation>
          <xs:documentation>Operation failed</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
    </xs:restriction>
  </xs:simpleType>

  <xs:complexType name="type.log.entry">
    <xs:annotation>
      <xs:documentation>Log entry format for log.file</xs:documentation>
    </xs:annotation>
    <xs:sequence>
      <xs:element name="record_number" type="xs:unsignedInt" />
      <!-- mandatory; unique identifier of this log entry -->
      <xs:element name="datetime" type="xs:dateTime" />
      <!-- mandatory; FAU_GEN/SYS.1.2 a), FAU_GEN/CON.1.2 a), FAU_GEN/CAL.1.2 a) -->
      <xs:element name="level" type="smgwlog:type.loglevel" />
      <!-- mandatory; -->
      <xs:element name="event_type" type="xs:string" />
```

```
        <!-- mandatory; FAU_GEN/SYS.1.2 a), FAU_GEN/CON.1.2 a), FAU_GEN/CAL.1.2 a) -->
        <xs:element name="subject_identity" type="xs:string" minOccurs="0" />
        <!-- optional; FAU_GEN/SYS.1.2 a), FAU_GEN/CON.1.2 a), FAU_GEN/CAL.1.2 a) -->
        <xs:element name="outcome" type="smgwlog:type.outcome" />
        <!-- mandatory; FAU_GEN/SYS.1.2 a), FAU_GEN/CON.1.2 a), FAU_GEN/CAL.1.2 a) -->
        <xs:element name="message" type="xs:string" />
        <!-- mandatory; FAU_GEN/SYS.1.2 b), FAU_GEN/CON.1.2 b), FAU_GEN/CAL.1.2 b) -->
        <xs:element name="user_identity" type="xs:string" minOccurs="0" />
        <!-- optional; FAU_GEN.2.1 -->
        <xs:element name="destination" type="xs:string" minOccurs="0" />
        <!-- optional; FCO_NRO.2 -->
        <xs:element name="evidence" type="xs:string" minOccurs="0" />
        <!-- optional; FCO_NRO.2 -->
      </xs:sequence>
    </xs:complexType>

    <xs:element name="log.file">
      <xs:annotation>
        <xs:documentation>
          Log file records for smart meter gateway
          (system-,consumer-,calibration-log)
        </xs:documentation>
      </xs:annotation>
      <xs:complexType>
        <xs:sequence>
          <xs:element name="log_entry" type="smgwlog:type.log.entry" minOccurs="0"
            maxOccurs="unbounded" />
        </xs:sequence>
        <xs:attribute name="LogfileReference" type="xs:string" use="required">
        </xs:attribute>
      </xs:complexType>
    </xs:element>
  </xs:schema>
```

5.2 Initialisierung

- technische Umsetzung, Kommunikationsfluß
- Zusammenspiel zwischen GW und Sicherheitsmodul

5.3 Administratorbefehle/ Managementbefehle

5.4 Sonstige funktionale Anforderungen (sofern nötig)

6 Nicht-Funktionale Anforderungen

6.1 Einleitung

Dieses Kapitel hat informativen Charakter.

Neben den funktionalen Anforderungen an ein Smart Metering System, die in Kapitel 3 beschrieben wurden, existiert eine Reihe von nicht-funktionalen Anforderungen, die in den folgenden Kapiteln dargestellt werden.

6.2 Versiegelung

Das Gateway **MUSS** sich gegen Angriffe schützen, die einen lokalen Zugriff auf das Gateway voraussetzen. Gemäß [GW_PP] gilt hierbei allerdings, dass das unterstellte Angriffspotential in diesem Szenario limitiert ist.

Beim Schutz, der durch das Gehäuse bereitgestellt wird, kann zwischen dem primären Gehäuse des Gateways und einem sekundären Gehäuse, das im Betrieb die Kommunikation zwischen einem Zähler und dem Gateway schützt unterschieden werden. Sofern nicht anders bezeichnet, gelten die Anforderungen im Folgenden für beide Gehäusearten.

Als Grundsatz kann festgehalten werden, dass durch eine Versiegelung dasselbe Schutzlevel erreicht werden **MUSS**, wie dies bei klassischen Zählern durch die Versiegelung bzw. Verwendung einer Plombe erreicht wird. Dieser Level wird durch spezifische Aspekte des Gateways ergänzt und durch die Anforderungen in diesem Kapitel beschrieben.

Das Gateway **MUSS** durch Verwendung eines geeigneten Siegels physische Manipulationen erkennbar machen. Es **DARF NICHT** möglich sein, das Gehäuse des Gateways zu öffnen ohne die Siegel erkennbar zu brechen.

Die Siegel **MÜSSEN** auf dafür geeigneten Siegelflächen angebracht werden, so dass sie im normalen Betrieb nicht durch Abnutzung gebrochen werden.

Die Siegel **MÜSSEN** im Sichtbereich des Anwenders liegen so dass sie ohne Werkzeug und direkt einer Sichtprüfung unterzogen werden können.

Die Siegel **MÜSSEN** durch das BSI freigegeben sein (siehe [TL 034xx]).

Das Gehäuse des Gateways **MUSS** geeignet sein, um unbemerkte Manipulationen ohne Bruch der Siegel zu verhindern. Insbesondere **MUSS** das Gehäuse mit Ausnahme der notwendigen Schnittstellen vollständig geschlossen sein und **DARF KEINE** Öffnungen besitzen, durch die eine Manipulation möglich ist.

Die Siegel auf das primäre Gehäuse **MÜSSEN** in der gesicherten Produktionsumgebung des Herstellers angebracht werden. Die Siegel dürfen dabei durch den Hersteller selbst angebracht werden.

Besitzt ein Gateway Schnittstellen, die nach außen zugänglich sind und über die eine ungesicherte Kommunikation erfolgen kann, **MÜSSEN** diese Schnittstellen durch ein sekundäres Gehäuse gesichert werden. Sobald das Gateway die Produktionsumgebung beim Hersteller verlässt, **MÜSSEN** solche Schnittstellen mit einem eindeutigen Warnhinweis versehen werden, dass das Gateway nur in einer durch eine sekundären Hülle geschützten Umgebung betrieben werden darf.

Die Versiegelung des sekundären Gehäuses **KANN** während der Installation geschehen. Dieser Vorgang **MUSS** durch geschultes Personal erfolgen und **MUSS** dokumentiert werden.

Das Gateway **SOLL** durch ein entsprechendes Design der Platine derart gestaltet sein, dass eine Manipulation von wichtigen Bauteilen erschwert wird.

Das Gateway **SOLL** über geeignete Mechanismen das Öffnen des Gehäuses detektieren können und für den Fall der Öffnung geeignet reagieren. Mindestens **SOLL** für den Fall einer Gehäuseöffnung der Administrator kontaktiert werden. Ferner **SOLL** das Ereignis im Eich-Log und System-Log protokolliert werden.

Dieser Mechanismus kann durch mechanische oder magnetische Kontakte, Lichtsensoren, eine Kombination der vorgenannten Mechanismen oder andere, geeignete Mechanismen realisiert werden.

6.3 Einbau des Sicherheitsmoduls

Das Sicherheitsmodul des Gateways enthält die kryptographische Identität des Gateways in Form des Schlüsselmaterials, das zur Authentisierung erforderlich ist und dient dem Gateway als kryptografischer Service Provider. Das Sicherheitsmodul **MUSS** daher fest mit dem Gateway verbunden sein (z.B. durch Verlötung).

Auch aus [PP_GW] leitet sich die Anforderung her, dass das Gateway sein Sicherheitsmodul und die Übertragungsstrecke zum Sicherheitsmodul physisch schützen muss.

Daher **MUSS** das Sicherheitsmodul fest in das Gateway eingebaut werden. Es **SOLL** wenn möglich ferner mit der Platine des Gateways derart vergossen werden (z.B. durch die Verwendung eines entsprechenden Harzes), dass ein Kontaktieren des Moduls geeignet erschwert wird.

Der Einbau des Sicherheitsmoduls **MUSS** während der Produktion des Gateways innerhalb der geschützten Produktionsumgebung erfolgen. Diese Produktionsumgebung **MUSS** derjenigen Umgebung entsprechen, die durch die Common Criteria Evaluation des Gateways betrachtet wurde.

6.4 QoS / Verfügbarkeit

6.5 Sonstige nicht-funktionale Anforderungen (sofern nötig)

7 Anforderungen zum Betrieb beim Administrator

7.1 Betriebsprozesse

7.1.1 Beschaffung und Produktion

- Zusammenspiel GW-Operator, GW-Hersteller, SM-Hersteller

7.1.2 Installation

7.1.3 Wartung

7.1.4 Zerstörung

7.1.5 Weiteres…

7.2 Sicherheitstechnische Anforderungen

- Betrieb der IT (Grundschutz?)

7.2.1 Betrieb eines Zeitdienstes

- Anforderungen an den Betrieb
- Wie synchronisiert sich der GW-Admin mit PTB-Zeitserver?

Literaturverzeichnis

[AIS20] AIS 20, Version 1, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, 02.12.1999

[AIS31] Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, 25.09.2001

[ANSIX9.62] American National Standards Institute, "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", ANS X9.62-2005, November 2005.

[CompNetz] Andrew S. Tanenbaum: Computernetzwerke, ISBN 3-8273-7046-9

[EN13757-4] Kommunikationssysteme für Zähler und deren Fernablesung Teil 4: Zählerauslesung über Funk (Fernablesung von Zählern im SRD-Band von 868 MHz bis 870 MHz), DIN, Deutsche Fassung EN 13757-4:2005

[EnWG] Energiewirtschaftsgesetz vom 7. Juli 2005 (BGBl. I S. 1970, 3621), Stand: Zuletzt geändert durch Art. 2 G v. 28.7.2011 I 1690

[FIPS197] NIST, FIPS 197, "Advanced Encryption Standard (AES)", November 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[GW_PP] Protection Profile for the Gateway of a Smart Metering System, BSI-CC-PP-0073

[ISO7498-1] Information technology – Open Systems Interconnection – Basic Reference Model: The basic model.

[ISO7816-4] International Standard ISO/IEC 7816-4, Identification cards – Integrated circuit cards -, Part 4: Organization, security and commands for interchange, Second edition 2005-01-15

[NIST SP800-38A] NIST, „Recommendation for Block Cipher Modes of Operation, Methods and Techniques“, NIST Special publication 800-38A, 2001 Edition

[OMS-1] Open Metering System Specification, Volume 1, General Part, OMS, Issue 1.4.0 / 2011-01-31

[OMS-2] Open Metering System Specification, Volume 2, Primary Communication, OMS, Issue 3.0.1 / 2011-01-29

[OMS-3] Open Metering System Specification, Volume 3, Tertiary Communication and OMS-MUC, OMS, Issue 2.0.0 / 2011-01-31

[PKCS#7] PKCS #7: Cryptographic Message Syntax Version 1.5, RFC 2315, March 1998.

[PKCS1] Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1", RFC 3447, February 2003.

[RFC2119] S. Bradner, “Key words for use in RFCs to Indicate Requirement Levels”, RFC 2119, March 1997

[RFC2104] [HMAC] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, February 1997

[RFC2818] E. Rescorla, “HTTP Over TLS”, RFC 2818, May 2000.

[RFC4493] JH. Song, J. Lee, and T. Iwata, “The AES-CMAC Algorithm”, RFC 4493, June 2006

[RFC5639] M. Lochter, and J. Merkle, „Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation”, RFC 5639, March 2010

[RFC5905] Network Time Protocol Version 4: Protocol and Algorithms Specification, RFC 5095, June 2010

[RFC5906] Network Time Protocol Version 4: Autokey Specification, RFC 5906, June 2010.

[SM_PP] Protection Profile for the Security Module of a Smart Metering System

[TLS] T. Dierks, E. Rescorla, „The Transport Layer Security (TLS) Protocol Version 1.1”, RFC4346, April 2006

[TLS_ECC] E. Rescorla, “TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)“, RFC 5289, August 2008

[TR-02102] Bundesamt für Sicherheit in der Informationstechnik, „BSI-Technische Richtlinie kryptographische Verfahren: Empfehlungen und Schlüssellängen“, BSI TR-02102, Version 1.0, 2008-06-20

[TR-03111] Bundesamt für Sicherheit in der Informationstechnik, „Technical Guideline TR-03111 Elliptic Curve Cryptography“, BSI TR-03111, Version 1.11

Stichwort- und Abkürzungsverzeichnis

Fehler! Keine Indexeinträge gefunden.

Anhang A: Kryptographische Vorgaben

Anhang B: Das Sicherheitsmodul eines Smart Metering Systems

Anhang C: Public Key Infrastruktur