Anforderungskatalog

Ende-zu-Ende-Sicherheit für Smart Metering

Im Auftrag von Oesterreichs Energie, Brahmsplatz 3, 1041 Wien

Ausgeführt vom European Network for Cyber Security, Regulusweg 5, 2516 AC Den Haag, Niederlande

Version:	2023-1.0
Herausgeber:	Projektgruppe Ende-zu-Ende-Sicherheit Smart Metering
Datum:	07. Dezember 2023
Seiten:	91

Haftungsausschluss

Trotz sorgfältiger Prüfung kann keine Gewähr für die Richtigkeit der Inhalte übernommen werden. Mit Ausnahme von Vorsatz und grober Fahrlässigkeit übernimmt der Herausgeber und Medieninhaber keine Haftung für den Inhalt dieses Dokuments.

Medieninhaber:
Österreichs E-Wirtschaft
1040 Wien, Brahmsplatz 3
Tel.: +43 1 501 98- 0
Fax: +43 1 501 98- 900
info@oesterreichsenergie.at,
www.oesterreichsenergie.at

AUTOREN: PG END2END SECURITY SMART METERING, Oesterreichs Energie

MAARTEN HOEVE, European Network for Cyber Security (Projektleitung ENCS)

WOLFGANG LÖW, EVN AG (Projektleitung PG)
STEFAN AUER, Salzburg Netz GmbH
JOHANN BERNHARDT, Netz Burgendland GmbH
CHRISTIAN BLANK, Illwerke VKW AG
CHRISTOPH EBERL, Wiener Netze GmbH
BERNHARD EGGER, Netz Oberösterreich GmbH
HELMUT GADERBAUER, LINZ NETZ GmbH
CHRISTIAN HAISJACKL, TINETZ-Tiroler Netze GmbH
PIA HOSCHEK, Wiener Netze GmbH
GUSTAV KRAIGHER, KNG-Kärnten Netz GmbH
MICHAEL KREMSER, Stadtwerke Klagenfurt AG
LUKAS LAUSEGGER, Stadtwerke Klagenfurt AG
THOMAS LEITNER, LINZ NETZ GmbH
PHILIPP MEYER, IKB AG
TOBIAS NEBEL, Stromnetz Graz GmbH & Co KG
ANDREAS ORLITSCH, Energie Steiermark AG
THOMAS PFEIFFER, LINZ NETZ GmbH
THOMAS RATZENBÖCK, LINZ NETZ GmbH
ELVIRA SÁNCHEZ ORTIZ, ENCS
ALOIS SCHAFFERHOFER, Stromnetz Graz GmbH & Co KG
RENE SCHMID, Stadtwerke Klagenfurt AG
ARMIN SELHOFER, Österreichs Energie
MICHAEL SIMMER, Linz AG Telekom
BERND SINT, TINETZ-Tiroler Netze GmbH
ANDREA STEINBAUER, Energie Steiermark AG

Inhaltsverzeichnis

A. Aufbau

A.1 Geltungsbereich

Dieser Katalog beschreibt die Mindestanforderungen für Ende-zu-Ende-gesichertes Smart Metering in Österreich. Diese Anforderungen gelten für Hersteller bei Ausschreibungsverfahren für Smart Meter, (Hybrid-)Gateway, Zentrales System und ihre Kommunikationsverbindungen. Die Anwendung der Ende-zu-Ende-Sicherheit entspricht den empfohlenen Maßnahmen der von der E-Control Austria (ECA) am 27. Februar 2014 vorgelegten Risikoanalyse [1] für die Informationssysteme der Elektrizitätswirtschaft.

Der Begriff *Smart Metering* ist nicht mit dem Begriff *Smart Grid* zu verwechseln; die Sicherheit von Steuerungs- und Telekommunikationssystemen für die Stromübertragung und -verteilung ist beispielsweise nicht Teil dieses Anforderungskatalogs. Die zugrunde liegende Ende-zu-Ende-Sicherheitsarchitektur für Smart Metering wird in Kapitel B beschrieben.

Die Maßnahmen dieses Katalogs orientieren sich am aktuellen Stand der Technik in der IKT-Sicherheit, d.h. der Sicherheit der Informations- und Kommunikationstechnik. Ziel der IKT-Sicherheit ist es, die Authentizität und Integrität von Informationen im digitalen Datenverkehr[1] zu gewährleisten und vertrauliche Daten geheim zu halten. Die Begriffe *"sicher"*, " *gesichert"* und "*Sicherheit"* sind in diesem Katalog im Kontext der IKT-Sicherheit zu verstehen. Andere Auslegungen, wie *Sicherheit* im Sinne von Betriebssicherheit oder Unfallverhütung, sind ausdrücklich gekennzeichnet.

Dieses Dokument beschreibt die Anforderungen der Netzbetreiber an Hersteller und Lieferanten bei der Ausschreibung von Geräten und Systemen, die im Smart Metering mit Ende-zu-Ende-Sicherheit eingesetzt werden.

A.2 Wortlaut

Um zwischen normativem und informativem Inhalt zu unterscheiden, folgt dieser Anforderungskatalog der Terminologie der Technischen Richtlinie TR-03109 (z.B. [2], Abschnitt 1.5) des deutschen Bundesamtes für Sicherheit in der Informationstechnik. Schlüsselwörter werden in Übereinstimmung mit RFC2119 in Großbuchstaben gedruckt [3]:

- MUSS bedeutet, dass die Anforderung verpflichtend ist.
- DARF NICHT / DARF KEIN / DARF WEDER ... NOCH bedeuten den Ausschluss einer Eigenschaft/von Eigenschaften.
- SOLL beschreibt eine ausdrückliche Empfehlung. Abweichungen von den empfohlenen Spezifikationen müssen begründet werden.

[1] Der digitale Datenverkehr sollte im Zusammenhang mit der Ende-zu-Ende-Architektur von Smart Metering verstanden werden (siehe Kapitel B).

- SOLL NICHT kennzeichnet eine ausdrückliche Empfehlung, eine Eigenschaft auszuschließen. Abweichungen von den empfohlenen Spezifikationen müssen begründet werden.
- KANN / DARF bedeutet, dass die Eigenschaften optional sind.

A.3 Aufbau der Anforderungen

Jede Anforderung ist mit einem Anforderungskennzeichen (Anf._ID) gekennzeichnet und besteht aus den folgenden drei Punkten:

1. Anforderung
2. Empfehlung und Anleitung zur Umsetzung
3. Empfohlene Qualitätssicherungsmaßnahme

Diese sind wie folgt definiert:

1. Anforderung: Eine *Anforderung* beschreibt eine Anforderung oder Erwartung, die obligatorisch ist. In dieser Ausschreibungsunterlage wird der Begriff *Anforderung* im Sinne einer normativen, d.h. zwingenden Anforderung verwendet.

2. Empfehlung und Anleitung zur Umsetzung: Eine *Empfehlung* beschreibt Möglichkeiten, wie eine Anforderung umgesetzt werden kann. Eine Anforderung kann äquivalent gelöst werden, solange die äquivalente Methode ausführlich schriftlich begründet wird. Die *Anleitungen zur Umsetzung* enthalten Beispiele und Erläuterungen, wie die Anforderung auszulegen ist.

3. Empfohlene Qualitätssicherungsmaßnahme: Die *empfohlenen Qualitätssicherungs-maßnahmen* enthalten Vorschläge, wie die Anforderung geprüft werden soll. Ziel ist es, Empfehlungen sowohl für die Prüforganisation als auch für den Hersteller zu geben und den Hersteller über die zu erwartenden Prüfverfahren zu informieren. Diese empfohlenen Prüfverfahren werden in Anhang B ausführlich erläutert.

A.4 Anwendbarkeit

Sofern nicht anders angegeben, gelten die Anforderungen für den Zähler, das (Hybrid-)Gateway und das Zentrale System.

Die Anforderungen an die Sicherheit der im Zentralen System eingesetzten Software sind als Grundlage zu verstehen und müssen durch die Sicherheitspolitik des Systembetreibers ergänzt werden.

Anforderungen mit einer ID, die auf ".M" endet, gelten speziell für den Zähler.

Anforderungen mit einer ID, die auf ".GW" endet, gelten speziell für das (Hybrid-)Gateway.

Anforderungen mit einer ID, die auf ".CS" endet, gelten speziell für das Zentrale System.

Verweise auf eine Gruppe sind mit einem Sternchen gekennzeichnet, z.B. SXR_01.*.

A.5 Gliederung

Die Anforderungen in diesem Dokument lassen sich in die folgenden Kategorien einteilen:

- Kapitel C betrifft die Anforderungen an das Smart-Metering-System. Dabei werden insbesondere die folgenden Bereiche abgedeckt:
    - Allgemeine Sicherheitsanforderungen
        - Zukunftssicher
        - Minimierung der Schnittstellen
        - Kryptographische Algorithmen
    - Integrität der Daten
    - Systemfestigkeit
    - Zugriffskontrolle
    - Vertraulichkeit
    - Audits und Protokolle
    - Produktlebenszyklus und Governance
- Anhang A enthält Beschreibungen ausgewählter Prozesse. Diese dienen als Beispiele dafür, wie ausgewählte Sicherheitsanforderungen im Sinne der Ende-zu-Ende-Sicherheit umgesetzt werden können. Die Prozesse sollten nicht in einem normativen Sinne interpretiert werden, sondern als Unterstützung für ein besseres Verständnis.
- Anhang B enthält ein Glossar der Begriffe und Abkürzungen.
- Anhang C enthält Hinweise auf Leitlinien und weiterführende Literatur.

B. Ende-zu-Ende-Sicherheitsarchitektur

B.1 Smart-Meter-Architektur

Die generische Architektur des Smart-Metering-Systems ist in Abbildung 1 dargestellt. Die Anzahl der Schnittstellen ist auf das notwendige Minimum beschränkt. Die Beschreibungen orientieren sich an den Vorgaben der österreichischen Intelligente Messgeräte-AnforderungsVO (IMA-VO).

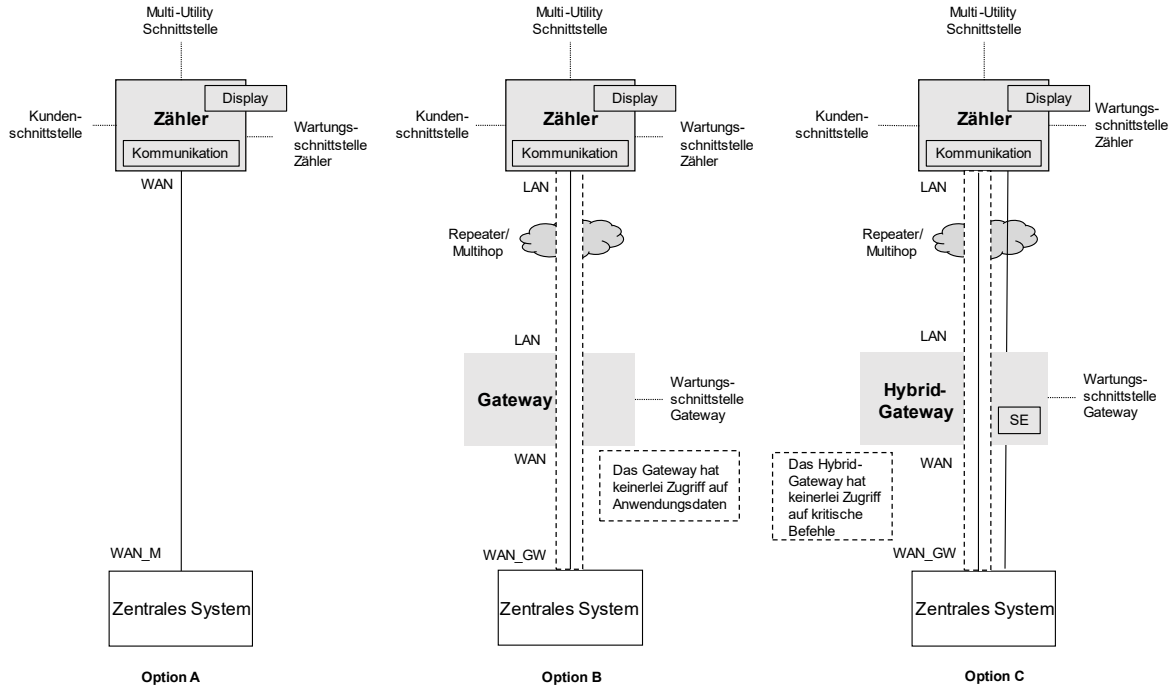

Abbildung 1: Ende-zu-Ende-Sicherheitsarchitektur für Smart Metering

Die Ende-zu-Ende-gesicherte Smart-Meter-Architektur berücksichtigt zwei Arten von Zählern. Der erste Typ sind Zähler, die über eine WAN-Schnittstelle mit dem Zentralen System verbunden sind. Der zweite Typ sind Zähler, die über ein lokales Netzwerk (LAN) mit einem Datenkonzentrator verbunden sind, der als Gateway zum Zentralen System fungiert.

Für die Sicherung der Kommunikation zwischen dem Zentralen System und dem Zähler sind drei verschiedene Möglichkeiten vorgesehen. Sie werden im Folgenden beschrieben. Bei all diesen Optionen müssen kritische Befehle an einzelne Zähler durchgängig gesichert werden. Ein Datenkonzentrator hat nicht die Berechtigung, Funktionen aufzurufen oder Einstellungen am Zähler zu ändern.

Aus diesem Grund wird der Begriff Hybrid-*Gateway* anstelle des Begriffs *Datenkonzentrator* verwendet.

Insbesondere ist zu beachten, dass bei den Optionen A und B das Gateway kein kryptografisches Schlüsselmaterial speichert, um Daten, die zwischen den Zählern und dem Zentralen System ausgetauscht werden, zu entschlüsseln, zu verändern oder zu analysieren. Bei Option C dürfen nur die Schlüssel für die Hybrid-Gateway-Rolle auf dem Hybrid-Gateway gespeichert werden, und diese sind durch ein sicheres Element geschützt.

Falls der Zähler und das WAN- oder LAN-Kommunikationsmodul durch physisch getrennte Komponenten realisiert werden, müssen die Schnittstellen zwischen diesen Komponenten ausschließlich mit den in diesem Dokument zugelassenen kryptografischen Methoden gesichert werden.

Für die Implementierung der Smart-Meter-Infrastruktur wird auch die Realisierung eines mehrschichtigen Sicherheitskonzepts empfohlen. Neben der durchgängig gesicherten Anwendungsschicht zwischen den Zählern und dem Zentralen System können auch kryptografische Verfahren zur Sicherung der unteren Kommunikationsschichten eingesetzt werden. Die Sicherheitsanforderungen für ein solches Konzept sind jedoch nicht Teil dieses Dokuments.

B.1.1 Option A: Direkt angeschlossenes Smart-Meter-System

Bei der Architekturoption A kommunizieren die intelligenten Zähler direkt mit dem Head-End-System über das WAN. Es wird davon ausgegangen, dass das WAN von einer anderen Partei als dem Netzbetreiber gewartet wird. Die Anforderungen beziehen sich nicht auf dieses Netz, sondern zielen auf Ende-zu-Ende-Sicherheit ab: Der intelligente Zähler und das Zentrale System können die Integrität und Vertraulichkeit der über das WAN gesendeten Daten gewährleisten, ohne von anderen Netzkomponenten im WAN abhängig zu sein. Die Verfügbarkeit hängt natürlich vom WAN ab.

B.1.2 Option B: Ende-zu-Ende-gesichertes Smart-Meter-System

Bei der Architekturoption B besitzt das Gateway keine Schlüssel und Berechtigungsnachweise der intelligenten Zähler, mit denen es kommuniziert, und kann die Daten, die es durchläuft, weder lesen noch ändern.

Die Anforderungen für Option B sind so gestaltet, dass die Kommunikation zwischen intelligenten Zählern und den Zentralen Systemen durchgängig sicher ist. In diesem Sinne entspricht Option B der Option A. Der Unterschied besteht darin, dass bei Option A alle Netzkomponenten von einer anderen Partei verwaltet werden, während bei Option B das Gateway vom Netzbetreiber verwaltet wird. Daher muss der Netzbetreiber Maßnahmen zu seiner Sicherung ergreifen. Daher sind Anforderungen für das Gateway enthalten.

B.1.3 Option C: Hybrider Ansatz

Bei Option C kann das Gateway Messdaten von Smart Metern auslesen, aber kritische Befehle (wie das Schalten des Unterbrechers, das Ändern von Schlüsseln oder das Aktualisieren der Firmware) werden von den Zentralen Systemen über eine sichere Ende-zu-Ende-Verbindung an den Smart Meter gesendet.

Der hybride Ansatz kann durch eine Trennung der Rollen auf dem Smart Meter umgesetzt werden, wie in Abschnitt B.3 unten beschrieben. Das Gateway erhält nur die Anmeldeinformationen für die *Hybrid-Gateway*-Rolle, so dass es nur Informationen vom Smart Meter abrufen kann. Es kann keine Einstellungen ändern oder kritische Befehle ausführen, wie z.B. die Aktivierung von Firmware-Aktualisierungen oder das Ändern von Schlüsseln.

Um das gleiche Sicherheitsniveau wie bei den Optionen A und B zu erreichen, sollte ein sicheres Element verwendet werden, um die Schlüssel, Kundendaten und andere Daten des Zählers, die auf dem Hybrid-Gateway gespeichert sind, zu schützen. Die Anforderungen an das sichere Element sind in Abschnitt C.8 enthalten.

Zähler:

Der Begriff *Zähler* bezieht sich auf den Stromzähler. An die Multi-Utility-Schnittstelle des Stromzählers können auch andere Versorgungszähler wie Gas, Wasser oder Wärme angeschlossen werden.

Kommunikation:	Der Zähler unterstützt entweder eine WAN- oder eine LAN-Schnittstelle.
Display:	Display bezieht sich auf die integrierte Anzeige des Zählers. Es gelten die Anforderungen der IMA-VO.
Kundenschnittstelle:	Die Kundenschnittstelle liefert dem Verbraucher aktuelle Verbrauchsinformationen gemäß der IMA-VO. Die Schnittstelle darf ausschließlich mit unidirektionaler Kommunikation implementiert werden.
Multi-Utility-Schnittstelle:	An die Multi-Utility-Schnittstelle des Stromzählers werden Zähler für die Versorgungsbereiche Gas, Wasser und Wärme angeschlossen.
Wartungsschnittstelle:	Der Zugriff auf den Stromzähler innerhalb der Eichstelle, in einem Prüflabor oder vor Ort durch einen Techniker erfolgt über die Wartungsschnittstelle am Stromzähler. Die Schnittstelle muss mit bidirektionaler Kommunikation implementiert werden.

LAN-Schnittstelle	Die LAN-Schnittstelle des Zählers stellt eine Verbindung zu einem Gateway und damit eine Verbindung zum Zentralen System her. Die Schnittstelle muss mit bidirektionaler Kommunikation implementiert werden.
WAN-Schnittstelle:	Die WAN-Schnittstelle des Zählers stellt eine direkte Verbindung zum Zentralen System her. Die Schnittstelle muss mit bidirektionaler Kommunikation implementiert werden.

(Hybrid-)Gateway:

Das Gateway ist die Komponente innerhalb der Smart-Metering-Architektur, die eine transparente Kommunikationsverbindung zwischen dem Zentralen System und dem Zähler herstellt. Transparent ist im Sinne einer Ende-Zu-Ende-Sicherheitsarchitektur zu verstehen.

Der Begriff *Gateway* kann als Teilfunktion eines Datenkonzentrators gesehen werden, der die Anforderungen einer Ende-zu-Ende-gesicherten Smart-Metering-Kommunikation widerspiegelt.

Wartungsschnittstelle:	Auf das Gateway kann ein Techniker innerhalb einer Prüforganisation oder im Feld über die Wartungsschnittstelle zugreifen. Die Schnittstelle muss mit bidirektionaler Kommunikation implementiert werden.
LAN-Schnittstelle:	Die LAN-Schnittstelle des Gateways stellt die Verbindung zwischen dem Gateway und den Zählern her. Die Schnittstelle muss mit bidirektionaler Kommunikation implementiert werden.
WAN-Schnittstelle:	Die WAN-Schnittstelle des Gateways stellt die Verbindung zum Zentralen System her. Die Schnittstelle muss mit bidirektionaler Kommunikation implementiert werden.

Zentrales System:

Das Zentrale System ist die zentrale Auslese- und Verwaltungsanwendung, die die Smart-Metering-Architektur nutzt und steuert.

WAN_GW-Schnittstelle:	Die WAN_GW-Schnittstelle des Gateways stellt die Verbindung zum Zentralen System her. Die Schnittstelle muss mit bidirektionaler Kommunikation implementiert werden.

WAN_M-Schnittstelle: Die WAN_M-Schnittstelle des Zentralen Systems stellt direkte Verbindungen zu den Zählern her. Die Schnittstelle muss mit bidirektionaler Kommunikation implementiert werden.

B.2 Architektur des Zentralen Systems

Abbildung 2 beschreibt die Architektur des Zentralen Systems. Die Anzahl der Schnittstellen ist auf das notwendige Minimum beschränkt. Die Pfeile zeigen an, ob eine Schnittstelle unidirektionale oder bidirektionale Kommunikation implementiert.

Das Zentrale System umfasst Head-End, MDMS und ein Key-Management-System für die Smart-Meter-Infrastruktur. Das Kundenportal ist nicht Teil des Zentralen Systems.

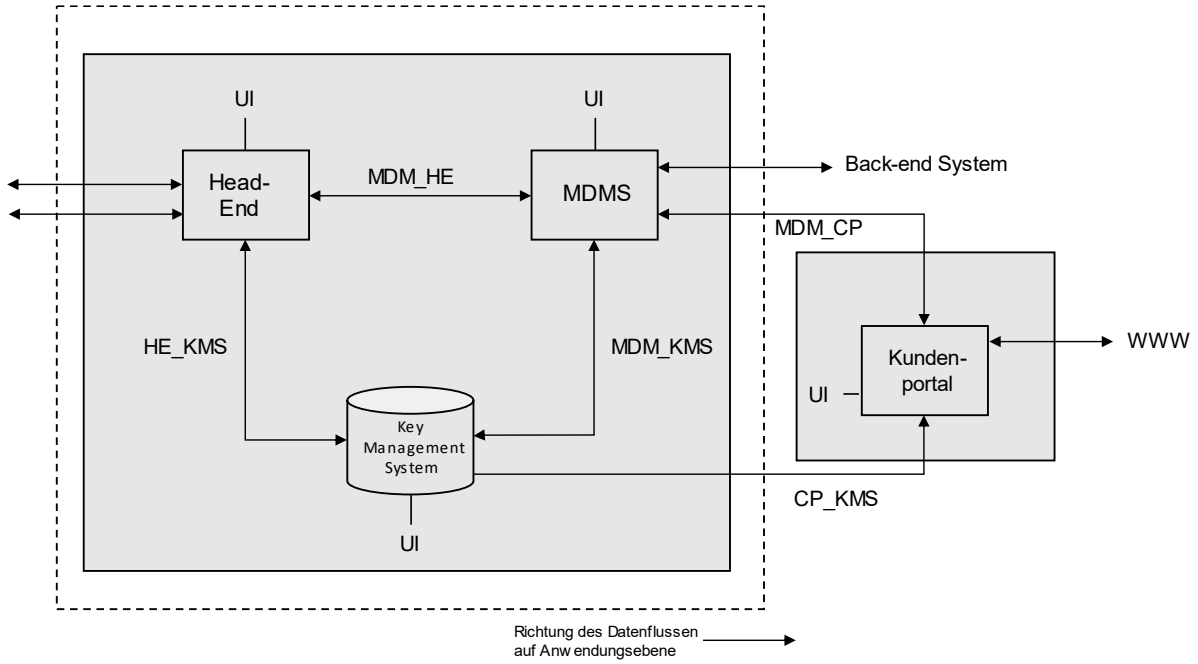

Abbildung 2: Architektur des Zentralen Systems

Head-End-System:

Das Head-End-System kommuniziert mit den Stromzählern und dem (Hybrid-)Gateway, liefert Daten an das Meter Data Management System (MDMS) und leitet Nachrichten vom MDMS an die Zähler weiter.

Benutzeroberfläche (UI): Über diese Schnittstelle werden die operativen und Wartungsarbeiten am Head-End-System abgewickelt. Die Benutzeroberfläche kann auch eine Fernwartungsschnittstelle enthalten.

HE_KMS-Schnittstelle: Über diese Schnittstelle kann das Head-End-System mit dem Key-Management-System kommunizieren.

MDM_HE-Schnittstelle: Das Head-End-System und das Meter-Data-Management-System kommunizieren über die MDM_HE-Schnittstelle.

Meter-Data-Management-System:

Das Meter-Data-Management-System (MDMS) speichert, verarbeitet und verwaltet die Zählerdaten und stellt diese Daten für das Kundenportal und die internen Betriebsprozesse zur Verfügung. Der MDMS kann auch Funktionen wie die Ersatzwertbildung oder die Verwaltung von Firmware-Dateien übernehmen.

Benutzeroberfläche (UI): Über diese Schnittstelle werden die operativen und Wartungsarbeiten am Head-End-System abgewickelt. Die Benutzeroberfläche kann auch eine Fernwartungsschnittstelle enthalten. In diesem Fall sollten die Betreiber auf der Grundlage einer Risikobewertung zusätzliche Anforderungen in Betracht ziehen, z.B. die Verwendung einer Zwei-Faktor-Authentifizierung oder eines Jump-Servers.

Back-End-System-Schnittstelle: Diese Schnittstelle verbindet das Meter-Data-Management-System mit dem internen Back-End-System für die internen Betriebsabläufe. Das Back-End-System kann Systeme zur Analyse und Speicherung von Netzqualitätsinformationen von den Zählern enthalten.

MDM_HE-Schnittstelle: Das Head-End-System und das Meter-Data-Management-System kommunizieren über die MDM_HE-Schnittstelle.

MDM_KMS-Schnittstelle: Diese Schnittstelle ermöglicht dem MDMS die Kommunikation mit dem Key-Management-System.

Key-Management-System:

Das Key-Management-System (KMS) verwaltet und schützt kryptografische Schlüssel. Das KMS bietet eine sichere Speicherung von Schlüsselmaterial und eine Zugangskontrolle für die Verwendung des Schlüsselmaterials. Werden Zertifikate verwendet, kann das KMS als Zertifizierungsstelle für die Public-Key-Infrastruktur fungieren. Das Key-Management-System sollte aus unabhängigen Komponenten bestehen, z.B. aus einer Komponente für das Head-End und einer separaten Komponente für das Kundenportal.

Benutzeroberfläche (UI):	Über diese Schnittstelle werden Wartungsarbeiten am Head-End-System abgewickelt. Wird der Fernzugriff über diese Schnittstelle genutzt, sollten strenge Maßnahmen zur Verhinderung und Erkennung von unbefugtem Zugriff getroffen werden.
HE_KMS-Schnittstelle:	Das Head-End-System und das Key-Management-System kommunizieren über die HE_KMS-Schnittstelle.
MDM_KMS-Schnittstelle:	Diese Schnittstelle ermöglicht dem MDMS die Kommunikation mit dem Key-Management-System.
KP_KMS-Schnittstelle:	Das Kundenportal und das Key-Management-System kommunizieren über die KP_KMS-Schnittstelle.

Kundenportal:

Das Kundenportal (KP) ist in dieser Architektur als das Kundenportal des Netzbetreibers und nicht eines Dritten zu verstehen. Das Kundenportal bietet Zugang für Kunden und autorisierte Dritte. Das Kundenportal ist der einzige Bereich, der über das öffentliche Internet zugänglich ist. Das Kundenportal ist nicht Teil des Zentralen Systems. Dieses Dokument enthält keine detaillierten Sicherheitsspezifikationen für das Kundenportal.

Benutzeroberfläche (UI):	Über diese Schnittstelle werden Wartungsarbeiten am Kundenportal abgewickelt. Die Benutzeroberfläche kann auch eine Fernwartungsschnittstelle enthalten.
Web-Schnittstelle (WWW):	Die Webschnittstelle ist die Verbindung zum öffentlichen Internet. Über diese Schnittstelle können Kunden und Dritte auf das Kundenportal zugreifen.
KP_KMS-Schnittstelle:	Das Kundenportal und das Key-Management-System können über die KP_KMS-Schnittstelle kommunizieren, um die auf der Kundenschnittstelle des Zählers verwendeten Schlüssel in das Kundenportal zu exportieren. Die Kommunikation ist einseitig in dem Sinne, dass das Key-Management-System dem Kundenportal nicht erlauben sollte, Schlüssel zu ändern. Es sollten Maßnahmen, wie z.B. die Verwendung von Proxys, ergriffen werden, um das Key-Management-System vor Angriffen über das Kundenportal zu schützen. Das Kundenportal kann auch indirekt mit dem Key-

Management-System kommunizieren, zum Beispiel über das MDMS.

MDM_KP-Schnittstelle: Das Meter-Data-Management-System und das Kundenportal kommunizieren über die MDM_KP-Schnittstelle. Die Kommunikation kann unidirektional sein, um das MDMS gegen ein beschädigtes Kundenportal zu schützen.

Back-End-System-Schnittstelle: Diese Schnittstelle verbindet das Kundenportal mit dem internen Back-End-System für interne Betriebsabläufe.

B.3 Rollen

In diesem Abschnitt werden Rollen und zugehörige Berechtigungen für rollenbasierte Zugriffskontrollrollen im Hinblick auf die beschriebene Architektur definiert. Die Anzahl der Rollen für die in der Architektur definierten Komponenten ist auf das notwendige Minimum beschränkt. Die vorgeschlagenen Privilegien sind beispielhaft. Die endgültigen Berechtigungseinstellungen sind vom Netzbetreiber festzulegen.

B.3.1 Rollen am Zähler

Rolle	Berechtigungen	Anwendbarkeit	Zähler-Schnittstellen
Eichung und Prüfung	Aufgaben der Rolle *Eichung und Prüfung*: Zugang für Eichstelle, externe Validierungsstelle, Marktüberwachung, Sachverständige oder Zertifizierungsstelle ermöglichen. Berechtigungen der Rolle *Eichung und Prüfung*: Aus-Schalter einstellen, Messung konfigurieren, Messregister lesen, Tarife einstellen, Firmware-Aktualisierung durchführen, Zugriff auf Protokoll-Dateien, Parametrierung und Konfiguration.	Internes Eichlabor des Netzbetreibers, externe Validierungsstelle, Marktüberwachung, Zertifizierungsstelle	Wartungs-schnittstelle
Wartung	Aufgaben der Rolle *Wartung*: Konfiguration des Geräts vor Ort. Berechtigungen der Rolle *Wartung*: Firmware-Aktualisierung, Auslesen von Messregistern, Konfiguration (z.B. Einstellen der Uhrzeit, Kopplung mit Versorgungszählern (Gas, Wärme, Wasser)), Einstellen des Ausschalters.	Handbediengerät, Service-Anwendung	Wartungs-schnittstelle

Installation	Aufgaben der Rolle *Installation*: Inbetriebnahme und Installation des Zählers durch einen Techniker vor Ort. Berechtigungen der Rolle *Installation*: Firmware-Aktualisierung, Auslesen von Messregistern, Konfiguration (z.B. Einstellen der Uhrzeit, Kopplung mit Versorgungszählern (Gas, Wärme, Wasser)). Diese Rolle sollte deaktiviert werden, sobald der Zähler erfolgreich in Betrieb genommen wurde. Die Reaktivierung der Rolle darf nur mit einem gesicherten Befehl möglich sein.	Handbediengerät, Service-Anwendung	Wartungs-schnittstelle
Kunde	Aufgaben der Rolle *Kunde*: Unidirektionale Kundenschnittstelle zur Anzeige von Verbrauchsdaten. Berechtigungen der Rolle *Kunde*: Register mit den aktuellen Verbrauchsdaten lesen, wie von der IMA-VO gefordert. Hinweis: Der Zugriff auf die Registerwerte kann ohne Eingabe durch den Kunden erfolgen, z.B. ist es möglich, Verbrauchsdaten permanent auf die Kundenschnittstelle zu senden.	Kundenschnittstelle	Kunden-schnittstelle

Display[2]	Aufgaben der Rolle *Display*: Ermöglicht das Lesen von Informationen, die auf dem Display angezeigt werden. Die Berechtigung der Rolle *Display* beschränkt sich ausschließlich auf die aktuell auf dem Zählerdisplay zugänglichen Informationen. Beispiele sind aktuelle Verbrauchswerte, Firmware-Version oder Seriennummer. Die Rolle *Display* kann ohne Benutzerauthentifizierung implementiert werden.	Handbediengerät, externe Validierungsstelle, Marktüberwachung	Wartungs-schnittstelle
Zentrales System Nur Lesen	Die *Nur-Lesen-Rolle* hat Lesezugriff auf definierte Speicherbereiche (Register, Ladeprofile usw.).	Zentrales System	WAN oder LAN
Zentrales System Lesen-Schreiben	Die Rolle *Lesen-Schreiben* hat Zugriff auf alle Speicherbereiche und Funktionen. Diese Rolle kann die Privilegien aller Rollen ändern.	Zentrales System	WAN oder LAN

[2] Die Rolle *Display* ist nicht zu verwechseln mit der Anzeige des Zählers. Die Rolle *Display* hat Zugriffsrechte auf die gleichen Daten, die lokal über das Display des Zählers zugänglich sind.

Hybrid-Gateway *(nur bei Option C)*	Die Rolle *Hybrid-Gateway* hat nur die folgenden Rechte: • Lesen von Verbrauchsdaten • Lesen von Netzqualitätsdaten • Lesen von Protokolldateien • Hochladen von Firmware (das Aktivieren der Firmware ist nicht erlaubt) • Zeitsynchronisation für Driftkompensation Die Rolle sollte die Zeit nur um bis zu 10 Minuten pro Tag ändern dürfen, damit ein kompromittiertes Hybrid-Gateway einen Zähler nicht dazu verleiten kann, ein abgelaufenes Zertifikat zu akzeptieren. Das *Hybrid-Gateway* hat keine anderen Zugriffsberechtigungen.	Hybrid-Gateway	LAN

B.3.2 Rollen am (Hybrid-)Gateway

Rolle	**Berechtigungen**	**Anwendbarkeit**	**Gateway-Schnittstellen**
Wartung	Aufgaben der Rolle *Wartung*: Konfiguration des Geräts vor Ort. Berechtigungen der Rolle *Wartung*: Firmware-Aktualisierungen, Auslesen von Protokolldateien, Konfiguration (z.B. Zeit einstellen).	Handbediengerät, Service-Anwendung	Wartungs-schnittstelle
Zentrales System Nur Lesen	Die *Nur-Lesen*-Rolle hat Lesezugriff auf definierte Speicherbereiche (Konfigurations- oder Protokolldateien).	Zentrales System	WAN

Zentrales System Lesen-Schreiben	Die Rolle *Lesen-Schreiben* hat Zugriff auf alle Speicherbereiche und Funktionen. Diese Rolle kann die Privilegien aller Rollen ändern.	Zentrales System	WAN

B.3.3 Rollen am Zentralen System

In diesem Abschnitt werden Rollen und zugehörige Berechtigungen für rollenbasierte Zugriffskontrollrollen im Hinblick auf die beschriebene Architektur definiert. Die Anzahl der Rollen für die in der Architektur definierten Komponenten ist auf das notwendige Minimum beschränkt. Die vorgeschlagenen Privilegien sind beispielhaft. Die endgültigen Berechtigungseinstellungen sind vom Netzbetreiber festzulegen.

Head-End-System

Rolle	**Berechtigungen**	**Anwendbarkeit**	**Schnittstellen Zentrales System**
Head-End-Wartung	Die Rolle *Head-End-Wartung* kann das Head-End konfigurieren.	Head-End	Benutzer-oberfläche
MDMS	Das MDMS verwendet die Rolle *MDMS* für die Benutzerauthentifizierung am Head-End.	Head-End	MDM_HE
Bediener Nur Lesen	Der Benutzer mit der Rolle *Bediener Nur Lesen* kann Daten von angeschlossenen Zählern oder (Hybrid-)Gateways auslesen.	Head-End	Benutzer-oberfläche
Bediener Lesen-Schreiben	Der Benutzer mit der Rolle *Bediener Lesen-Schreiben* kann Daten von angeschlossenen Zählern oder	Head-End	Benutzer-oberfläche

	(Hybrid-)Gateways auslesen und schreiben.		

MDM-System

Rolle	Berechtigungen	Anwendbarkeit	Schnittstellen Zentrales System
Head-End	Das Head-End verwendet die *Rolle Head-End* für die Benutzerauthentifizierung am MDMS.	MDMS	MDM_HE
MDMS-Wartung	Die Rolle *MDMS-Wartung* kann das MDMS konfigurieren. Insbesondere kann diese Rolle festlegen, welche Informationen an das Kundenportal und an das Back-End-System weitergeleitet werden dürfen.	MDMS	Benutzer-oberfläche
Bediener Nur Lesen	Der Benutzer mit der Rolle *Bediener Nur Lesen* kann Daten vom MDMS auslesen.	MDMS	Benutzer-oberfläche
Bediener Lesen-Schreiben	Der Benutzer mit der Rolle *Bediener Lesen-Schreiben* kann Daten im MDMS auslesen und schreiben.	MDMS	Benutzer-oberfläche

Kundenportal

Rolle	Berechtigungen	Anwendbarkeit	Schnittstellen Zentrales System
Kunde	Die Rolle *Kunde* kann auf einen oder mehrere Datensätze im Kundenportal zugreifen. Jedem Kunden und Dritten wird eine individuelle Rolle zugewiesen.	Kundenportal	Internet

Wartung Kundenportal	Die Rolle *Wartung Kundenportal* kann das Kundenportal konfigurieren.	Kundenportal	Benutzer-oberfläche
MDMS_KP	Das MDMS verwendet die Rolle *MDMS_KP* für die Benutzerauthentifizierung am Kundenportal.	Kundenportal	MDM_KP

Key-Management-System

Rolle	Berechtigungen	Anwendbarkeit	Schnittstellen Zentrales System
KMS-Wartung	Die Rolle *KS-Wartung* kann das Key-Management-System konfigurieren.	Key-Management-System	Benutzer-oberfläche
Kundenportal	Das Kundenportal verwendet die Rolle *Kundenportal* für die Benutzerauthentifizierung am KMS.	Key-Management-System	KP_KMS
Head-End	Das Head-End verwendet die *Rolle Head-End* für die Benutzerauthentifizierung am KMS.	Key-Management-System	HE_KMS
MDMS	Das Meter-Data-Management-System verwendet die Rolle *MDMS* für die Benutzerauthentifizierung am KMS.	Key-Management-System	MDM_KMS

B.4 Sicherheitsrelevante Ereignisse

Jedes Sicherheitsereignis sollte, wenn möglich, den Zeitpunkt, die Benutzer- oder Systemidentifikation (ID), die Schnittstellen sowie das Ergebnis des Ereignisses protokollieren.

Zähler und Gateway sollten mindestens die folgenden Ereignistypen unterstützen:

Ereignis	Gerät

Protokollierung einer erfolgreichen oder fehlgeschlagenen Benutzerauthentifizierung für eine bestimmte Rolle.	Zähler und (Hybrid-)Gateway
Firmware-Aktualisierungen • Protokollierung von erfolgreichen Firmware-Aktualisierungen. • Protokollierung von fehlgeschlagenen Firmware-Aktualisierungen aufgrund ungültiger digitaler Signaturen. • Unterscheidung zwischen dem Empfang eines Firmware-Images und der Aktivierung einer Firmware-Aktualisierung.	Zähler und (Hybrid-)Gateway
Einstellung der Systemzeit.	Zähler und (Hybrid-)Gateway
Ereignisse, die von Manipulationserkennungssensoren registriert werden. Dazu gehört z.B. das Öffnen von Geräteabdeckungen.	Zähler und (Hybrid-)Gateway
Starten des Geräts (Bootvorgang).	Zähler und (Hybrid-)Gateway
Zurücksetzen oder Neustart des Geräts.	Zähler und (Hybrid-)Gateway
Zurücksetzen von Fehler- oder Ereignisregistern oder der zugehörigen Protokolldateien.	Zähler und (Hybrid-)Gateway
Protokollierung von Gerätefehlern. Siehe Anforderungen SRR_02.*.	Zähler und (Hybrid-)Gateway
Rekonfiguration der kryptographischen Parameter. Zum Beispiel: • Aktualisierung des kryptografischen Schlüsselmaterials für eine ausgewählte Rolle. • Änderung der Zugriffsrechte für eine ausgewählte Rolle. • Zurücksetzen des Zufallszahlengenerators (Seed).	Zähler und (Hybrid-)Gateway
Aus-Schalter: ein/aus.	Zähler
Ereignisse im Zusammenhang mit Versorgungszählern: • Gerätepaarung von Versorgungszähler und Stromzähler • Aktualisierung des kryptografischen Schlüsselmaterials für den Versorgungszähler	Zähler
Änderung der Parameter der Lastbegrenzung	Zähler

C. Sichere Zählerkommunikation

C.1 Allgemeine Sicherheitsanforderungen

C.1.1 Zukunftssicher

Anf._ID	
SFR_01.M	**Anforderung**
	Der Zähler MUSS über genügend Speicher (flüchtig und nichtflüchtig) und Rechenleistungsreserven verfügen, um Aktualisierungen der Sicherheitsfunktionen zu ermöglichen. Die Aktualisierbarkeit MUSS während des gesamten Produktlebenszyklus gewährleistet sein.
	Empfehlung und Anleitung zur Umsetzung
	1. Der Hersteller SOLL den Nachweis erbringen, dass ausreichende Reserven für die Aktualisierung der Sicherheitsfunktionen vorhanden sind. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist. 2. Dazu gehören insbesondere kryptographische Algorithmen und Kommunikationsprotokolle. Bitte beachten Sie SPR_01. 3. Der Zähler SOLL über Speicherplatz verfügen, der ausschließlich für die Aktualisierung der Sicherheitsfunktionen reserviert ist. 4. Wenn DLMS verwendet wird, SOLL der Zähler die Aktualisierung auf Suite 1 und Suite 2 für kryptografische Algorithmen unterstützen, wenn diese noch nicht implementiert sind.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Es wird empfohlen, die vom Hersteller bereitgestellten Konstruktionsunterlagen zu analysieren.
SFR_01.GW	Anforderung
	Das (Hybrid-)Gateway MUSS über ausreichend Speicher (flüchtig und nichtflüchtig) und Rechenleistungsreserven verfügen, um Aktualisierungen der Sicherheitsfunktionen zu ermöglichen.

	Die Aktualisierbarkeit MUSS während des gesamten Produktlebenszyklus gewährleistet sein.
	Empfehlung und Anleitung zur Umsetzung
	1. Der Hersteller SOLL den Nachweis erbringen, dass ausreichende Reserven für die Aktualisierung der Sicherheitsfunktionen vorhanden sind. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist. 2. Dazu gehören vor allem kryptographische Algorithmen und Kommunikationsprotokolle. Bitte beachten Sie SPR_01. 3. Das (Hybrid-)Gateway SOLL über Speicherplatz verfügen, der ausschließlich für die Aktualisierung der Sicherheitsfunktionen reserviert ist. 4. Wenn DLMS verwendet wird, SOLL das (Hybrid-)Gateway die Aktualisierung auf Suite 1 und Suite 2 für kryptografische Algorithmen unterstützen, wenn diese noch nicht implementiert sind.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Es wird empfohlen, die vom Hersteller bereitgestellten Konstruktionsunterlagen zu analysieren.
SFR_01.CS	**Anforderung**
	Das Zentrale System MUSS Aktualisierungen der Sicherheitsfunktionen unterstützen. Wenn kryptografische Algorithmen im KMS implementiert sind, MUSS es möglich sein, diese zu aktualisieren. Die Aktualisierbarkeit MUSS während des gesamten Produktlebenszyklus gewährleistet sein.
	Empfehlung und Anleitung zur Umsetzung
	1. Der Hersteller SOLL den Nachweis erbringen, dass ausreichende Reserven für die Aktualisierung der Sicherheitsfunktionen vorhanden sind. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist. 2. Dazu gehören insbesondere kryptographische Algorithmen und Kommunikationsprotokolle. Bitte beachten Sie SPR_01.

	3. Wenn DLMS verwendet wird, SOLL das Zentrale System ein Upgrade auf Suite 1 und Suite 2 für kryptografische Algorithmen unterstützen, wenn diese noch nicht implementiert sind.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Es wird empfohlen, die vom Hersteller bereitgestellten Konstruktionsunterlagen zu analysieren.
SFR_02.M	**Anforderung**
	Der Zähler MUSS es ermöglichen, dass alle Teile der Firmware, die kryptografische Algorithmen, externe Kommunikation und Messtechnik implementieren, durch lokale und Remote-Firmware-Aktualisierungen aktualisiert werden können.
	Empfehlung und Anleitung zur Umsetzung
	1. Siehe auch Anforderung SPR_01.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Es wird empfohlen, die vom Hersteller bereitgestellten Konstruktionsunterlagen zu analysieren. 2. Es wird empfohlen, einen Fuzzing-Test der Firmware-Aktualisierungsfunktionen durchzuführen.
SFR_02.GW	**Anforderung**
	Das (Hybrid-)Gateway MUSS es ermöglichen, dass alle Teile der Firmware, die kryptografische Algorithmen und die externe Kommunikation implementieren, durch lokale und Remote-Firmware-Aktualisierungen aktualisiert werden können.
	Empfehlung und Anleitung zur Umsetzung
	1. Siehe auch Anforderung SPR_01.

	2. Fernaktualisierungen des (Hybrid-)Gateways SOLLEN durch Fern-Aktualisierungen der Firmware oder Fern-Patching erfolgen.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Es wird empfohlen, die vom Hersteller bereitgestellten Konstruktionsunterlagen zu analysieren. 2. Es wird empfohlen, einen Fuzzing-Test der Firmware-Aktualisierungsfunktionen durchzuführen.
SFR_03.M	**Anforderung**
	Der Zähler MUSS die Fähigkeit unterstützen, lokal und aus der Ferne zu aktualisieren oder zu widerrufen: • alle Berechtigungen der jeweiligen Rollen • alle kryptografischen Schlüssel • öffentliches Schlüsselmaterial, das für die Validierung der digital signierten Firmware-Aktualisierungen verwendet wird Der Zähler MUSS die Aktualisierung der für die Kommunikation verwendeten kryptografischen Schlüssel ohne Unterstützung durch den Hersteller ermöglichen. Die Integrität und Vertraulichkeit der Schlüssel MUSS bei Aktualisierungen geschützt sein.
	Empfehlung und Anleitung zur Umsetzung
	1. Zu den Anforderungen an die rollenbasierte Zugangskontrolle siehe Abschnitt C.4. 2. Für die Aktualisierung kryptografischer Schlüssel SOLL ein authentifiziertes Schlüsselaustauschprotokoll verwendet werden, um ihre Integrität zu schützen. Beim Einsatz der Public-Key-Kryptografie SOLL das Gerät in der Lage sein, neue Schlüsselpaare zusammen mit einer Zertifikatsignierungs-anfrage zu erzeugen. Beim Einsatz der Public-Key-Kryptografie SOLL der Zähler in der Lage sein, neue Zertifikate zu importieren. 3. Berechtigungen und öffentliche Schlüssel, die zum Signieren der Firmware verwendet werden, können durch Firmware-Aktualisierungen aktualisiert werden.

	Empfohlene Qualitätssicherungsmaßnahme
	1. Diese Anforderung wird durch einen funktionalen Sicherheitstest überprüft.
SFR_03.GW	**Anforderung**
	Das (Hybrid-)Gateway MUSS die Fähigkeit unterstützen, aus der Ferne zu aktualisieren oder zu widerrufen • alle Berechtigungen der jeweiligen Rollen • alle kryptografischen Schlüssel • öffentliches Schlüsselmaterial, das für die Validierung der digital signierten Firmware-Aktualisierungen verwendet wird Die Integrität und Vertraulichkeit der Schlüssel MUSS bei Aktualisierungen geschützt sein.
	Empfehlung und Anleitung zur Umsetzung
	1. Zu den Anforderungen an die rollenbasierte Zugangskontrolle siehe Abschnitt C.4. 2. Für die Aktualisierung kryptografischer Schlüssel SOLL ein authentifiziertes Schlüsselaustauschprotokoll verwendet werden, um ihre Integrität zu schützen. 3. Beim Einsatz der Public-Key-Kryptografie SOLL das Gerät in der Lage sein, neue Schlüsselpaare zusammen mit einer Zertifikatsignierungs-anfrage zu erzeugen. Beim Einsatz von Public-Key-Kryptographie SOLL das (Hybrid-)Gateway in der Lage sein, neue Zertifikate zu importieren.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Diese Anforderung wird durch einen funktionalen Sicherheitstest überprüft.
SFR_03.CS	**Anforderung**

	Das Zentrale System MUSS die Fähigkeit unterstützen, die Berechtigungen der jeweiligen Rollen sowie die kryptografischen Schlüssel zu aktualisieren oder zu widerrufen.
	Empfehlung und Anleitung zur Umsetzung
	1. Zu den Anforderungen an die rollenbasierte Zugangskontrolle siehe Abschnitt C.4. 2. Zum Schutz der Integrität von kryptographischem Schlüsselmaterial siehe SIR_01.CS.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Diese Anforderung wird durch einen funktionalen Sicherheitstest überprüft.

C.1.2 Minimierung der Schnittstellen

Anf._ID	
SMR_01	**Anforderung**
	Jede Schnittstelle DARF nur die Funktionen und Protokolle unterstützen, die zur Erfüllung der funktionalen Anforderungen erforderlich sind. Debugging- oder Analysefunktionen, die während des Entwicklungsprozesses verwendet werden, MÜSSEN bei Produktionszählern deaktiviert werden.
	Empfehlung und Anleitung zur Umsetzung
	1. Der Hersteller SOLL den Nachweis erbringen, dass nur die beschriebene Funktionalität implementiert ist. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist. 2. Der Hersteller SOLL eine vollständige Liste der unterstützten Datentypen und der unterstützten Kommunikationsprotokolle bereitstellen. 3. Beispiele für Debugging- oder Analysefunktionen sind: Webserver eines (Hybrid-)Gateways, die während der Entwicklungsphase als Debugging-Tool verwendet werden, oder spezielle Tastenkombinationen zum

	Aufrufen eines technischen Menüs eines Zählers, das sicherheitsrelevante Änderungen ermöglicht.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Die Durchführung eines Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung angemessen umgesetzt wurde.
SMR_02	**Anforderung**
	Deaktivierte oder nicht genutzte Funktionen DÜRFEN die Sicherheit NICHT beeinträchtigen.
	Empfehlung und Anleitung zur Umsetzung
	1. Der Hersteller SOLL den Nachweis erbringen, dass erforderliche Zusatzfunktionen die Sicherheit nicht beeinträchtigen; Zusatzfunktionen sind Funktionen, die über die betrieblichen Aufgaben und die regelmäßige Kommunikation zwischen dem Zähler und dem Zentralen System hinausgehen. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist. 2. Funktionen, die deaktiviert sind und auf dem Gerät nie benötigt werden, SOLLEN vollständig entfernt werden. 3. Deaktivierte Funktionalität sollte weder über undokumentierte Funktionen noch über undefinierte oder fehlerhafte Betriebszustände ansprechbar sein. ○ Beispiele für ungenutzte Funktionen sind in der Firmware enthaltene Routinen, die im normalen Betriebsmodus nicht verwendet werden. ○ Weitere Beispiele sind Prüf- und Debugging-Funktionen, die zur Initialisierung während des Produktionsprozesses verwendet werden.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Die Durchführung eines Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung angemessen umgesetzt wurde. 2. Es wird empfohlen, vom Hersteller einen Nachweis über die Codeüberprüfung zu verlangen.

C.1.3 Kryptographische Algorithmen

Anf._ID	
SPR_01	**Anforderung**
	1. Der Hersteller MUSS bei der Verwendung von kryptografischen Primitiven und Schlüssellängen die neueste Version der folgenden Leitlinien befolgen: • NIST SP 800-57 Teil 1 Rev. 5, Empfehlung für die Schlüsselverwaltung: Teil 1 - Allgemeines [4] oder eine neuere Version. • BSI TR-03116, Teil 3, "Kryptographische Vorgaben für Projekte der Bundesregierung - Intelligente Messsysteme" [5]. Nur Kapitel 2 "Kryptographische Algorithmen" und Kapitel 4.2.1 "Cipher Suites und Kurvenparameter" in der referenzierten Version 2023 [5] sind anwendbar.[3] 2. Der Hersteller DARF WEDER proprietäre kryptografische Funktionen verwenden NOCH die in Punkt 1 genannten kryptografischen Primitive verändern.
	Empfehlung und Anleitung zur Umsetzung
	1. BSI TR-02102-1 "Kryptographische Verfahren: Empfehlungen und Schlüssellängen" [6] gibt Auskunft über den Stand der Technik in der Kryptographie. 2. Der Hersteller SOLL den Nachweis so detailliert erbringen, dass eine einfache Überprüfung möglich ist. 3. Siehe SFR_01.* bezüglich des erforderlichen Speichers für die Aktualisierung der kryptografischen Funktionen. 4. Bei der Verwendung von Zertifikaten SOLL eine vertrauenswürdige Zeit oder Zeitquelle in den verwendeten Systemen/Geräten gewährleistet sein.

[3] Beachten Sie, dass insbesondere die BSI-Anforderungen zur Sicherung des HAN mittels TLS nicht Teil der in diesem Dokument beschriebenen Zählerarchitektur sind.

	5. In einigen Fällen kann es erforderlich sein, Algorithmen, die nach den oben genannten Leitlinien nicht mehr zulässig sind, die Kommunikation mit älteren Geräten zu ermöglichen. In diesem Fall SOLL eine Risikobewertung durchgeführt werden, um festzustellen, ob die älteren Geräte aktualisiert werden sollten oder ob die älteren Algorithmen auf den neu beschafften Geräten zugelassen werden können.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Diese Anforderung wird in einem funktionalen Sicherheitstest überprüft. 2. Es wird empfohlen, die vom Hersteller bereitgestellten Konstruktionsunterlagen zu analysieren.
SPR_02	**Anforderung**
	Alle sicherheitsrelevanten Zufallswerte MÜSSEN von kryptographischen Zufallszahlengeneratoren gemäß AIS 20 erzeugt werden [7], AIS 31 [8] oder gleichwertig.
	Empfehlung und Anleitung zur Umsetzung
	1. Der Hersteller SOLL den Nachweis erbringen, dass diese Anforderung erfüllt ist. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist. 2. Sicherheitsrelevante Zufallswerte werden z.B. für die Generierung von digitalen Signaturen, kryptographischen Schlüsseln oder Authentifizierungsprotokollen verwendet. 3. FIPS 186-4 [9] und FIPS 140-2 (Anhang C) [10] werden als gleichwertig mit den genannten Richtlinien angesehen.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Die Durchführung eines Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung angemessen umgesetzt wurde. 2. Es wird empfohlen, die vom Hersteller bereitgestellten Konstruktionsunterlagen zu analysieren.

C.2 Integrität der Daten

Anf._ID	
SIR_01.M	**Anforderung**
	Der Zähler MUSS die Authentizität und Integrität aller über die folgenden Schnittstellen empfangenen Daten überprüfen: • Multi-Utility-Schnittstelle zwischen dem Stromzähler und anderen Versorgungszählern • Wartungsschnittstelle • LAN zwischen dem Stromzähler und dem Zentralen System • WAN zwischen dem Stromzähler und dem Zentralen System Sowohl die Authentizität der Quelle (Absender) als auch die Authentizität der empfangenen Nachricht MUSS überprüft werden. Die Nachricht MUSS verworfen werden, wenn die Integrität des Absenders oder der Daten nicht überprüft werden kann.
	Empfehlung und Anleitung zur Umsetzung
	1. Nachrichten SOLLEN durch Anhängen eines Nachrichten-Authentifizierungscodes (MAC) authentifiziert werden. 2. Die Authentizität des Absenders kann durch die Prüfung der beigefügten gültigen digitalen Signatur überprüft werden. 3. In der Anforderung SPR_01 sind die zulässigen kryptografischen Algorithmen aufgeführt. 4. Im Zusammenhang mit der Ende-zu-Ende-Sicherheitsarchitektur betrifft diese Anforderung die Anwendungsschicht (OSI-Schichten 5-7).
	Empfohlene Qualitätssicherungsmaßnahme
	1. Der Hersteller SOLL einen Nachweis für die Implementierung der geforderten Funktionalität erbringen. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist. 2. Die Durchführung eines Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung angemessen umgesetzt wurde.

SIR_01.GW	**Anforderung**
	Das (Hybrid-)Gateway MUSS die Authentizität und Integrität der über die folgenden Schnittstellen empfangenen Daten überprüfen: • Wartungsschnittstelle • WAN-Schnittstelle zum Zentralen System, sofern die Daten nicht direkt an den Smart Meter weitergeleitet werden, • LAN-Schnittstelle zu den Smart Metern, sofern die Daten nicht direkt an das Zentrale System weitergeleitet werden. Sowohl die Authentizität der Quelle (Absender) als auch die Authentizität der empfangenen Nachricht MUSS überprüft werden. Die Nachricht MUSS verworfen werden, wenn die Integrität des Absenders oder der Daten nicht überprüft werden kann.
	Empfehlung und Anleitung zur Umsetzung
	1. Nachrichten SOLLEN durch Anhängen eines Nachrichten-Authentifizierungscodes (MAC) authentifiziert werden. 2. Die Authentizität des Absenders kann durch die Überprüfung einer beigefügten gültigen digitalen Signatur überprüft werden. 3. In der Anforderung SPR_01 sind die zulässigen kryptografischen Algorithmen aufgeführt. 4. Im Zusammenhang mit der Ende-zu-Ende-Sicherheitsarchitektur betrifft diese Anforderung die Anwendungsschicht (OSI-Schichten 5-7).
	Empfohlene Qualitätssicherungsmaßnahme
	1. Der Hersteller SOLL einen Nachweis für die Implementierung der geforderten Funktionalität erbringen. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist. 2. Die Durchführung eines Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung angemessen umgesetzt wurde.
SIR_01.CS	**Anforderung**
	Die Authentizität und Integrität der auf allen Schnittstellen empfangenen Daten und der zwischen den implementierten Zonen im Zentralen System verkehrenden Daten MUSS überprüft werden.

	Sowohl die Authentizität der Quelle (Absender) als auch die Authentizität der empfangenen Nachricht MUSS überprüft werden. Die Nachricht MUSS verworfen werden, wenn die Integrität des Absenders oder der Daten nicht überprüft werden kann.
	Empfehlung und Anleitung zur Umsetzung
	1. Die Anforderung SRR_04.CS enthält Einzelheiten zur Zoneneinteilung im Zentralen System. 2. Nachrichten SOLLEN durch Anhängen eines Nachrichten-Authentifizierungscodes (MAC) authentifiziert werden. 3. Die Authentizität des Absenders kann durch die Überprüfung einer beigefügten gültigen digitalen Signatur überprüft werden. 4. In der Anforderung SPR_01 sind die zulässigen kryptografischen Algorithmen aufgeführt. 5. Im Zusammenhang mit der Ende-zu-Ende-Sicherheitsarchitektur betrifft diese Anforderung die Anwendungsschicht (OSI-Schichten 5-7).
	Empfohlene Qualitätssicherungsmaßnahme
	1. Der Hersteller SOLL einen Nachweis für die Implementierung der geforderten Funktionalität erbringen. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist. 2. Die Durchführung eines Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung angemessen umgesetzt wurde.
SIR_02.M	**Anforderung**
	Der Zähler MUSS die Gültigkeit aller Datenpakete und das Format der an den folgenden Schnittstellen empfangenen Daten überprüfen: • Multi-Utility-Schnittstelle zwischen dem Stromzähler und anderen Versorgungszählern • Wartungsschnittstelle • LAN zwischen dem Stromzähler und dem Zentralen System • WAN zwischen dem Stromzähler und dem Zentralen System
	Empfehlung und Anleitung zur Umsetzung

	1. Sowohl das Gerätedesign als auch die Implementierung SOLLEN sicherstellen, dass die korrekte Funktion des Zählers nicht durch beschädigte oder absichtlich fehlerhafte Pakete beeinträchtigt wird. 2. Die Anforderung gilt für alle Schichten des OSI-Modells.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Es wird empfohlen, Fuzzing-Tests an den beschriebenen Schnittstellen durchzuführen. 2. Der Hersteller soll die durchgeführten Sicherheitstests so detailliert dokumentieren, dass eine Validierung möglich ist. Der Hersteller soll die durchgeführten Sicherheitstests in die Produktdokumentation aufnehmen.
SIR_02.GW	**Anforderung**
	Das (Hybrid-)Gateway MUSS die Gültigkeit aller Datenpakete und das Format der an den folgenden Schnittstellen empfangenen Daten überprüfen: • Wartungsschnittstelle • WAN-Schnittstelle zum Zentralen System, sofern die Daten nicht direkt an den Smart Meter weitergeleitet werden, • LAN-Schnittstelle zu den Smart Metern, sofern die Daten nicht direkt an das Zentrale System weitergeleitet werden.
	Empfehlung und Anleitung zur Umsetzung
	1. Sowohl das Gerätedesign als auch die Implementierung SOLLEN sicherstellen, dass die korrekte Funktion des (Hybrid-)Gateways nicht durch beschädigte oder absichtlich fehlerhafte Pakete beeinträchtigt wird. 2. Die Anforderung gilt für alle Schichten des OSI-Modells.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Es wird empfohlen, Fuzzing-Tests an den beschriebenen Schnittstellen durchzuführen. 2. Der Hersteller soll die durchgeführten Sicherheitstests so detailliert dokumentieren, dass eine Validierung möglich ist. Der Hersteller soll die

	durchgeführten Sicherheitstests in die Produktdokumentation aufnehmen.
SIR_02.CS	**Anforderung**
	Das Zentrale System MUSS die Gültigkeit aller Datenpakete und das Format der auf allen Schnittstellen empfangenen Daten sowie den Datenaustausch zwischen implementierten Zonen überprüfen.
	Empfehlung und Anleitung zur Umsetzung
	1. Die Anforderung SRR_04.CS enthält Einzelheiten zur Zoneneinteilung im Zentralen System. 2. Die Anforderung betrifft sowohl die externen als auch die internen Schnittstellen (Zone zu Zone). 3. Sowohl das Gerätedesign als auch die Implementierung SOLLEN sicherstellen, dass das Zentrale System nicht durch beschädigte oder absichtlich fehlerhafte Pakete beeinträchtigt wird. 4. Die SQL-Bereinigung ist eine Gegenmaßnahme zur SQL-Einschleusung; sie ist ein Beispiel für die Datenvalidierung im Zentralen System. Weitere Beispiele für die Datenvalidierung auf Webservern sind in der ÖNORM A 7700 beschrieben [11] und im OWASP-Kapitel "*Input Validation"* [12]. 5. Die Anforderung gilt für alle Schichten des OSI-Modells.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Es wird empfohlen, Fuzzing-Tests an den beschriebenen Schnittstellen durchzuführen. 2. Der Hersteller soll die durchgeführten Sicherheitstests so detailliert dokumentieren, dass eine Validierung möglich ist. Der Hersteller soll die durchgeführten Sicherheitstests in die Produktdokumentation aufnehmen.
SIR_03.M	**Anforderung**
	Der Zähler MUSS die Integrität von Firmware-Images überprüfen, bevor sie angewendet werden. • Der Hersteller MUSS die gesamte Firmware-Aktualisierung digital signieren.

	• Firmware-Aktualisierungen ohne gültige digitale Signatur MÜSSEN verworfen werden. • Die Firmware-Aktualisierung MUSS abgebrochen werden, wenn ihre Versionsnummer niedriger ist als die Versionsnummer der installierten Firmware. • Der Zähler MUSS das Downgrade auf eine ältere Firmware-Version unterstützen, wenn dies für den Betrieb erforderlich ist. Ein solches Downgrade MUSS unter einer neuen Versionsnummer importiert werden. • Daten auf dem Zähler (z.B. gespeicherte Zählerdaten, Protokolleinträge oder kundenspezifische Konfigurationen) DÜRFEN durch eine Firmware-Aktualisierung NICHT verändert oder gelöscht werden. • Wenn eine Firmware-Aktualisierung neue Funktionen installiert, MUSS die Funktion in einer sicheren Standardkonfiguration installiert werden. Alle neuen Parameter in der Firmware MÜSSEN auf sichere Werte initialisiert werden.
	Empfehlung und Anleitung zur Umsetzung
	1. Der ECDSA-Algorithmus mit einer zulässigen Schlüsselstärke SOLL zur Erzeugung einer digitalen Signatur verwendet werden. Siehe SPR_01. 2. Der öffentliche Schlüssel für die Validierung der digitalen Signatur SOLL während des Herstellungsprozesses auf dem Zähler installiert werden. Siehe Beispiel-Prozesse in Anhang A. 3. Digital signierte Firmware-Aktualisierungen können als Broadcast/Multicast verschickt werden. Siehe Beispiel-Prozesse in Anhang A. 4. Ein angemessenes Freigabemanagement des Firmware-Builds beim Hersteller SOLL sicherstellen, dass die digitale Signatur des Images vertrauenswürdig ist.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Die funktionale Anforderung soll durch Testen der implementierten Firmware-Aktualisierungsfunktionen überprüft werden. 2. Im Hinblick auf die Anforderungen an Prozesse können Sicherheitsaudits als Teil von Abnahme- oder Funktionstests durchgeführt werden.

	3. Sicherheitsaudits der Entwicklungs- und Firmware-Release-Prozesse können als Teil eines allgemeinen Sicherheitsaudits, z.B. nach ISO 27001, durchgeführt werden. 4. Durchführung eines Fuzzing-Tests, um zu überprüfen, ob die Funktionen der Firmware-Aktualisierung angemessen implementiert sind.
SIR_03.GW	**Anforderung**
	Das (Hybrid-)Gateway MUSS die Integrität von Firmware-Images überprüfen, bevor sie angewendet werden. • Der Hersteller MUSS die Firmware-Aktualisierung digital signieren. • Firmware-Aktualisierungen ohne gültige digitale Signatur MÜSSEN verworfen werden. • Die Firmware-Aktualisierung MUSS abgebrochen werden, wenn ihre Versionsnummer niedriger ist als die Versionsnummer der installierten Firmware. • Das (Hybrid-)Gateway MUSS das Downgrade auf eine ältere Firmware-Version unterstützen, wenn dies für den Betrieb erforderlich ist. Ein solches Downgrade MUSS unter einer neuen Versionsnummer importiert werden. • Daten auf dem (Hybrid-)Gateway (z.B. Protokolleinträge) DÜRFEN durch eine Firmware-Aktualisierung NICHT verändert oder gelöscht werden. Notwendige Änderungen an der Konfiguration der eingesetzten Funktionen MÜSSEN während des Aktualisierungsprozesses automatisch durchgeführt werden.
	Empfehlung und Anleitung zur Umsetzung
	1. Der ECDSA-Algorithmus mit einer zulässigen Schlüsselstärke SOLL zur Erzeugung einer digitalen Signatur verwendet werden. Siehe SPR_01. 2. Der öffentliche Schlüssel für die Validierung der digitalen Signatur SOLL während des Herstellungsprozesses auf dem (Hybrid-)Gateway installiert werden. Siehe Beispiel-Prozesse in Anhang A. 3. Digital signierte Firmware-Aktualisierungen können als Broadcast/Multicast verschickt werden. Siehe Beispiel-Prozesse in Anhang A.

	4. Ein angemessenes Freigabemanagement des Firmware-Builds beim Hersteller SOLL sicherstellen, dass die digitale Signatur des Images vertrauenswürdig ist.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Die funktionale Anforderung soll durch Testen der implementierten Firmware-Aktualisierungsfunktionen überprüft werden. 2. Im Hinblick auf die Anforderungen an Prozesse können Sicherheitsaudits als Teil von Abnahme- oder Funktionstests durchgeführt werden. 3. Sicherheitsaudits der Entwicklungs- und Firmware-Release-Prozesse können als Teil eines allgemeinen Sicherheitsaudits, z.B. nach ISO 27001, durchgeführt werden. 4. Es wird empfohlen, einen Fuzzing-Test durchzuführen, um zu überprüfen, ob die Funktionen zur Aktualisierung der Firmware angemessen implementiert sind.
SIR_03.CS	**Anforderung**
	Das Zentrale System MUSS die Integrität von Firmware-Images überprüfen, bevor sie angewendet werden. • Der Hersteller MUSS die Software-Aktualisierung digital signieren. • Software-Aktualisierungen ohne gültige digitale Signatur MÜSSEN verworfen werden. • Das Zentrale System MUSS das Downgrade auf eine ältere Firmware-Version unterstützen, wenn dies für den Betrieb erforderlich ist. Ein solches Downgrade MUSS unter einer neuen Versionsnummer importiert werden.
	Empfehlung und Anleitung zur Umsetzung
	1. Der ECDSA-Algorithmus mit einer zulässigen Schlüsselstärke SOLL zur Erzeugung einer digitalen Signatur verwendet werden. Siehe SPR_01. 2. Ein angemessenes Freigabemanagement des Software-Builds beim Hersteller SOLL sicherstellen, dass die digitale Signatur der Aktualisierung vertrauenswürdig ist.

	Empfohlene Qualitätssicherungsmaßnahme
	1. Die funktionale Anforderung soll durch Testen der implementierten Software-Aktualisierungsfunktionen überprüft werden. 2. Im Hinblick auf die Anforderungen an Prozesse können Sicherheitsaudits als Teil von Abnahme- oder Funktionstests durchgeführt werden. 3. Sicherheitsaudits der Entwicklungs- und Aktualisierungs-Release-Prozesse können als Teil eines allgemeinen Sicherheitsaudits, z.B. nach ISO 27001, durchgeführt werden.
SIR_04.M	**Anforderung**
	Der Zähler MUSS in der Lage sein, Wiedereinspielangriffe auf den folgenden Schnittstellen zu erkennen: • Multi-Utility-Schnittstelle zwischen dem Stromzähler und anderen Versorgungszählern • Wartungsschnittstelle • LAN zwischen dem Stromzähler und dem Zentralen System • WAN zwischen dem Stromzähler und dem Zentralen System Der Zähler MUSS Wiedereinspielung (replay) von Nachrichten verwerfen.
	Empfehlung und Anleitung zur Umsetzung
	1. Um Wiedereinspielangriffe zu verhindern, SOLLEN alle Nachrichten auf eine der folgenden Arten gesichert werden: • Sequenznummer (counter) • Authentifizierte Nonce Es ist wichtig, dass die Nonce mit einem MAC-Algorithmus authentifiziert wird. • Authentifizierte Verschlüsselung mit einer Methode wie AES-CBC-CMAC, AES-CCM oder AES-GCM.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Die Durchführung eines Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung angemessen umgesetzt wurde. 2. Es wird empfohlen, die vom Hersteller bereitgestellten Konstruktionsunterlagen zu analysieren.

SIR_04.GW	**Anforderung**
	Das (Hybrid-)Gateway MUSS in der Lage sein, Wiedereinspielangriffe auf den folgenden Schnittstellen zu erkennen: • WAN-Schnittstelle zum Zentralen System, sofern die Nachrichten nicht direkt an den Smart Meter weitergeleitet werden, • LAN-Schnittstelle zum Smart Meter, sofern die Nachrichten nicht direkt an das Zentrale System weitergeleitet werden, • Wartungsschnittstelle Das (Hybrid-)Gateway MUSS Wiedereinspielung (replay) von Nachrichten verwerfen.
	Empfehlung und Anleitung zur Umsetzung
	1. Um Wiedereinspielangriffe zu verhindern, SOLLEN alle Nachrichten auf eine der folgenden Arten gesichert werden: • Sequenznummer (counter) • Authentifizierte Nonce Es ist wichtig, dass die Nonce mit einem MAC-Algorithmus authentifiziert wird. • Authentifizierte Verschlüsselung mit einer Methode wie AES-CBC-CMAC, AES-CCM oder AES-GCM.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Die Durchführung eines Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung angemessen umgesetzt wurde. 2. Es wird empfohlen, die vom Hersteller bereitgestellten Konstruktionsunterlagen zu analysieren.
SIR_04.CS	**Anforderung**
	Das Zentrale System MUSS in der Lage sein, Wiedereinspielangriffe auf allen externen und internen Schnittstellen und zwischen implementierten Zonen (Zone zu Zone) zu erkennen. Das Zentrale System MUSS Wiedereinspielung (replay) von Nachrichten verwerfen.

	Empfehlung und Anleitung zur Umsetzung
	1. Um Wiedereinspielangriffe zu verhindern, SOLLEN alle Nachrichten auf eine der folgenden Arten gesichert werden: • Sequenznummer (counter) • Authentifizierte Nonce Es ist wichtig, dass die Nonce mit einem MAC-Algorithmus authentifiziert wird. • Authentifizierte Verschlüsselung mit einer Methode wie AES-CBC-CMAC, AES-CCM oder AES-GCM. 2. Die Verwendung von TLS oder eines VPN kann diese Funktionalität bieten. Siehe auch SPR_01.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Die Durchführung eines Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung angemessen umgesetzt wurde. 2. Es wird empfohlen, die vom Hersteller bereitgestellten Konstruktionsunterlagen zu analysieren.

C.3 Systemfestigkeit

Anf._ID	
SRR_01.M	**Anforderung**
	Der Zähler MUSS die Messfunktionalität von der Kommunikationsfunktionalität trennen, damit es die Strommessung auch bei Denial-of-Service-Angriffen auf die Kommunikation korrekt beibehält. Nicht sicherheitsrelevante Funktionen DÜRFEN die Sicherheit des Gesamtsystems NICHT beeinträchtigen. Der Hersteller MUSS den Nachweis für die Abschottung von Sicherheits- und Nicht-Sicherheitsfunktionen und -blöcken erbringen.
	Empfehlung und Anleitung zur Umsetzung

	1. Der Hersteller SOLL dokumentieren, dass der Zähler ausreichend in Funktionsblöcke unterteilt ist. 2. Ein Beispiel für die Trennung von Funktionsblöcken des Zählers ist die Trennung von Messtechnik und Kommunikation. Kommunikationsprobleme SOLLEN keine negativen Auswirkungen auf die Messtechnik haben.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Die Durchführung eines Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung angemessen umgesetzt wurde. 2. Die Durchführung eines Fuzzing-Tests wird empfohlen, um den Nachweis zu erbringen, dass sich die Funktionsblöcke des Zählers nicht gegenseitig beeinflussen.
SRR_01.GW	**Anforderung**
	Getrennte Funktionsblöcke des (Hybrid-)Gateways DÜRFEN sich NICHT gegenseitig negativ beeinflussen. Nicht sicherheitsrelevante Funktionen DÜRFEN die Sicherheit des Gesamtsystems NICHT beeinträchtigen. Der Hersteller MUSS den Nachweis für die Abschottung von Sicherheits- und Nicht-Sicherheitsfunktionen und -blöcken erbringen.
	Empfehlung und Anleitung zur Umsetzung
	1. Der Hersteller SOLL dokumentieren, dass das (Hybrid-)Gateway ausreichend in Funktionsblöcke unterteilt ist. 2. Ein Beispiel für die Trennung von Funktionsblöcken des (Hybrid-)Gateways ist der Speicherschutz von separaten Prozessen (z.B. Routing oder Fernzugriff).
	Empfohlene Qualitätssicherungsmaßnahme
	1. Die Durchführung eines Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung angemessen umgesetzt wurde.

	2. Die Durchführung eines Fuzzing-Tests wird empfohlen, um den Nachweis zu erbringen, dass sich die Funktionsblöcke des (Hybrid-)Gateways nicht gegenseitig beeinflussen.
SRR_02.M	Anforderung
	Der Zähler MUSS *ausfallsicher* sein. • Die Vertraulichkeit und Integrität der Daten und Gerätefunktionen des Zählers MUSS auch bei Ausfällen gewährleistet sein. • Der Zähler DARF nicht zulassen, dass die Zugangskontrolle bei Ausfällen aus der Ferne umgangen werden. • Der Zähler MUSS die Verfügbarkeit nach Softwareausfällen so schnell wie möglich wiederherstellen. Der Hersteller MUSS Nachweise und Prüfberichte vorlegen, aus denen hervorgeht, wie der Zähler auf die folgenden Ausfälle reagiert: • Spannungsabfall • Integritätsfehler, z.B. bei Einstellungen, Konfigurationen oder Protokolldateien • Fehler bei Selbsttests des Zählers • Fehler bei der Ausführung von kryptographischen Funktionen • Fehler bei der Validierung von Anmeldedaten • Fehler bei der Dateneingabe (falsches Datenformat, falsche Datenlänge, ungültige Befehle usw.) • Fehler bei der Verwendung der lokalen Tasten (zu schnelles oder gleichzeitiges Drücken der Tasten)
	Empfehlung und Anleitung zur Umsetzung
	1. Der Hersteller SOLL einen Nachweis erbringen, dass der Zähler ausfallsicher ist. 2. Dieses Problem kann durch die Implementierung einer Watchdog-Funktion gelöst werden, die es dem Zähler ermöglicht, im Falle eines Ausfalls einen sicheren Betriebszustand aufrechtzuerhalten. 3. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist.
	Empfohlene Qualitätssicherungsmaßnahme

	1. Es wird empfohlen, einen Penetrationstest durchzuführen, um die Robustheit der Konstruktion weiter zu gewährleisten. 2. Es wird empfohlen, die vom Hersteller bereitgestellten Konstruktionsunterlagen zu analysieren.
SRR_02.GW	**Anforderung**
	Das (Hybrid-)Gateway MUSS *ausfallsicher* sein. • Die Vertraulichkeit und Integrität der Daten und Gerätefunktionen des (Hybrid-)Gateways MUSS auch bei Ausfällen gewährleistet sein. • Das (Hybrid-)Gateway DARF nicht zulassen, dass die Zugangskontrolle bei Ausfällen aus der Ferne umgangen werden. • Das (Hybrid-)Gateway MUSS die Verfügbarkeit nach Softwareausfällen so schnell wie möglich wiederherstellen. Der Hersteller MUSS Nachweise und Prüfberichte vorlegen, aus denen hervorgeht, wie das (Hybrid-)Gateway auf die folgenden Ausfälle reagiert: • Spannungsabfall • Integritätsfehler, z.B. bei Einstellungen, Konfigurationen oder Protokolldateien • Fehler bei Selbsttests des Zählers • Fehler bei der Ausführung von kryptographischen Funktionen • Fehler bei der Validierung von Anmeldedaten • Fehler bei der Dateneingabe (falsches Datenformat, falsche Datenlänge, ungültige Befehle usw.)
	Empfehlung und Anleitung zur Umsetzung
	1. Der Hersteller SOLL einen Nachweis erbringen, dass das (Hybrid-)Gateway ausfallsicher ist. 2. Dieses Problem kann durch die Implementierung einer Watchdog-Funktion gelöst werden, die es dem (Hybrid-)Gateway ermöglicht, im Falle eines Ausfalls einen sicheren Betriebszustand aufrechtzuerhalten. 3. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist.
	Empfohlene Qualitätssicherungsmaßnahme

	1. Es wird empfohlen, einen Penetrationstest durchzuführen, um die Robustheit der Konstruktion weiter zu gewährleisten. 2. Es wird empfohlen, die vom Hersteller bereitgestellten Konstruktionsunterlagen zu analysieren.
SRR_02.CS	**Anforderung**
	Das Zentrale System MUSS *ausfallsicher* sein. • Die Vertraulichkeit und Integrität der Daten und Gerätefunktionen von Komponenten des Zentralen Systems MUSS auch bei Ausfällen gewährleistet sein. • Das Zentrale System DARF nicht zulassen, dass die Zugangskontrolle bei Ausfällen aus der Ferne umgangen werden. • Das Zentrale System MUSS die Verfügbarkeit nach Softwareausfällen so schnell wie möglich wiederherstellen. Der Hersteller MUSS Nachweise und Prüfberichte vorlegen, aus denen hervorgeht, wie der Zähler auf die folgenden Ausfälle reagiert: • Integritätsfehler, z.B. bei Einstellungen, Konfigurationen oder Protokolldateien • Fehler bei der Ausführung von kryptographischen Funktionen • Fehler bei der Validierung von Anmeldedaten • Fehler bei der Dateneingabe (falsches Datenformat, falsche Datenlänge, ungültige Befehle usw.)
	Empfehlung und Anleitung zur Umsetzung
	1. Der Hersteller SOLL einen Nachweis erbringen, dass das Zentrale System ausfallsicher ist. 2. Beispiele für relevante Fehler sind: • Integritätsfehler, z.B. bei Einstellungen, Konfigurationen oder Protokolldateien • Fehler bei der Ausführung von kryptographischen Funktionen • Fehler bei der Validierung von Anmeldedaten • Fehler bei der Dateneingabe (falsches Datenformat, falsche Datenlänge, ungültige Befehle usw.)

	3. Der Hersteller SOLL den Nachweis erbringen, welche relevanten Ausfälle abgedeckt sind und wie diese getestet wurden. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Es wird empfohlen, einen Penetrationstest durchzuführen, um die Robustheit der Konstruktion weiter zu gewährleisten. 2. Es wird empfohlen, die vom Hersteller bereitgestellten Konstruktionsunterlagen zu analysieren.
SRR_03.M	**Anforderung**
	Physische Manipulationen am Zähler MÜSSEN erkennbar sein. • Das Gehäuse des Zählers MUSS einen ausreichenden Schutz gegen physische Manipulationen bieten. • Das Gehäuse des Zählers MUSS nach Möglichkeit versiegelt sein. • Außerdem MUSS das Öffnen der Klemmenabdeckung und separat des Zählergehäuses durch geeignete Mittel wie Kontakte oder Sensoren erkannt werden. Jedes Öffnen der Klemmenabdeckung oder des Gehäuses MUSS ein Ereignis im Sicherheitsprotokoll erzeugen. • Wenn der Zähler über abnehmbare Teile verfügt, MUSS das Entfernen eines solchen Teils ein Ereignis im Sicherheitsprotokoll erzeugen. Es MUSS ein unabhängiger Penetrationstest der physischen Sicherheit durchgeführt werden.
	Empfehlung und Anleitung zur Umsetzung
	1. Das Sicherheitsprotokoll ist in Anforderung SLR_01.M definiert. 2. Der Hersteller SOLL den Nachweis erbringen, dass diese Anforderung erfüllt ist. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist. 3. Es SOLL möglich sein, das Gehäuse des Zählers und die Klemmenabdeckung zu versiegeln. 4. Die Penetrationstests SOLLEN über einen angemessenen Zeitraum von einem erfahrenen Prüfer durchgeführt werden.

	Empfohlene Qualitätssicherungsmaßnahme
	1. Es wird empfohlen, die bei den Penetrationstests festgestellten Schwachstellen zu analysieren.
SRR_03.GW	**Anforderung**
	Physische Manipulationen am (Hybrid-)Gateway MÜSSEN erkennbar sein. • Das Gehäuse MUSS einen ausreichenden Schutz gegen physische Manipulationen bieten. • Wenn das (Hybrid-)Gateway über abnehmbare Teile verfügt, MUSS das Entfernen eines solchen Teils ein Ereignis im Sicherheitsprotokoll erzeugen.
	Empfehlung und Anleitung zur Umsetzung
	1. Das Sicherheitsprotokoll ist in Anforderung SLR_01.GW definiert. 2. Der Hersteller SOLL den Nachweis erbringen, dass diese Anforderung erfüllt ist. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Die Durchführung eines Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung angemessen umgesetzt wurde.
SRR_04.CS	**Anforderung**
	1. Das Zentrale System MUSS die Trennung in mindestens die folgenden Zonen unterstützen: a. Head-End-System b. Key-Management-System (KMS) c. Meter-Data-Management-System (MDMS) 2. Es MUSS möglich sein, die Kommunikation zwischen den Zonen und zwischen den Zonen und externen Systemen zu begrenzen.
	Empfehlung und Anleitung zur Umsetzung
	1. Allgemeine Beispiele für Mechanismen zur Trennung von Zonen sind:

	• Firewalls: Eine Firewall kontrolliert den Informationsfluss zwischen zwei Komponenten. Beachten Sie, dass eine falsche Konfiguration von Firewalls katastrophale Folgen haben kann: Die Konfigurationsflexibilität, die eine Firewall bietet, kann leicht zu Fehlkonfigurationen führen, die einem Angreifer den Weg ebnen. • Netzwerk-Gateways[4]: Ein Gateway regelt, welche Komponenten miteinander kommunizieren dürfen. • Datendioden: Eine Datendiode sorgt dafür, dass der Verkehr nur in eine Richtung fließt. Die empfangende Seite hat keine Berechtigung, Daten an den Absender zu senden und kann daher nicht als Einstiegspunkt für einen Angriff missbraucht werden. Datendioden sind sicherer, aber auch viel weniger flexibel als Firewalls oder Gateways. • Mikrokernel: Ein Mikrokernel oder Hypervisor ermöglicht die Trennung von Prozessen und ermöglicht somit Zoning ohne Hardwaretrennung. 2. Wenn möglich, sollte die Trennfunktionalität als eigene Komponente implementiert werden.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Die Durchführung eines Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung angemessen umgesetzt wurde.
SRR_05.CS	**Anforderung**
	Das Zentrale System MUSS kryptografische Schlüssel in einer sicheren Umgebung eines Key-Management-Systems speichern. Diese gesicherte Umgebung MUSS mindestens der Stufe 3 von FIPS 140-2 entsprechen [13].
	Empfehlung und Anleitung zur Umsetzung
	1. Die Verwendung von kryptographischen Funktionen und Schlüsseln ist in SPR_01 beschrieben. 2. Die Verwendung von kryptografischen Schlüsseln außerhalb der gesicherten Umgebung SOLL auf ein Mindestmaß beschränkt werden.

[4] Der Begriff "Gateway" ist hier als ein klassisches Mittel zur Verbindung von Computernetzen zu verstehen.

	○ Die Prozesse SOLLEN so gestaltet sein, dass die Geräte nur die Schlüssel erhalten, die sie benötigen. Hybrid-Gateways SOLLEN also nur die Schlüssel für die an sie angeschlossenen Zähler erhalten, und Handbediengeräte oder mobile Geräte SOLLEN nur die Schlüssel erhalten, die zur Ausführung ihrer Arbeitsaufträge erforderlich sind. ○ Werden die Schlüssel auf Geräte außerhalb der Smart Meter exportiert, z.B. auf Handbediengeräte oder mobile Geräte, SOLLEN die Schlüssel nur für eine begrenzte Zeit nutzbar sein. Sie SOLLEN nach der Verwendung aus dem Gerät gelöscht und auf dem Zähler oder (Hybrid-)Gateway geändert werden. Der Zeitraum, in dem ein Schlüssel gültig bleiben darf, SOLL durch eine Risikobewertung bestimmt werden. ○ Das Zentrale System SOLL eine Begrenzung der Anzahl der Schlüssel durchsetzen, die ein Gerät wie ein Hybrid-Gateway oder ein Handbediengerät erhalten kann. 3. Die Schlüssel SOLLEN die gesicherte Umgebung NICHT unverschlüsselt verlassen. 4. Es SOLL möglich sein, innerhalb der gesicherten Umgebung neue kryptografische Schlüssel zu erzeugen. 5. Die Schnittstelle, die die gesicherte Umgebung und das Key-Management-System verbindet, SOLL einen offenen Schnittstellenstandard verwenden, wie z.B. PKCS #11 [14]. 6. Alle Schnittstellen der gesicherten Umgebung SOLLEN eindeutig dokumentiert sein. 7. Es SOLL möglich sein, die Intervalle für den Zugriff auf die gesicherten Daten zu begrenzen. 8. Es SOLL möglich sein, ausgewählte Daten (und vor allem Schlüssel) nach dem Vier-Augen-Prinzip zu sichern.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Es wird empfohlen, die vom Hersteller bereitgestellten Konstruktionsunterlagen und Zertifikate zu analysieren.
SRR_06.CS	**Anforderung**
	Die Zentralen Systeme MÜSSEN vor Bedrohungen geschützt werden, die vom Kundenportal ausgehen. Es DARF nicht möglich sein, die Integrität der Informationen im MDMS über das Kundenportal zu beeinträchtigen.

	Empfehlung und Anleitung zur Umsetzung
	1. Die Betreiber SOLLEN die Sicherheitsanforderungen für das Kundenportal auf der Grundlage einer Risikobewertung festlegen. Das Kundenportal fällt nicht in den Anwendungsbereich der Anforderungen dieses Dokuments.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Es wird empfohlen, einen Penetrationstest durchzuführen, um die Robustheit der Konstruktion weiter zu gewährleisten.

C.4 Zugriffskontrolle

Anf._ID	
SAR_01.M	**Anforderung**
	Der Zähler MUSS rollenbasierte Zugriffskontrollen (Role Based Access Controls, RBAC) unterstützen, um das Gerät vor unbefugtem Zugriff zu schützen, indem unterschiedliche Zugriffsrechte auf der Grundlage der Rolle eines Benutzers durchgesetzt werden. • Der Zähler MUSS die Implementierung des in Abschnitt B.3.1 definierten Rollenmodells ermöglichen. • Es MUSS möglich sein, die Berechtigungen der einzelnen Rollen zu konfigurieren. • Es MUSS möglich sein, jeder Rolle individuelles Schlüsselmaterial zuzuordnen. Diese Schlüssel MÜSSEN aktualisierbar sein. • Es MUSS möglich sein, Rollen an Schnittstellen zu binden. • Es MUSS möglich sein, weitere Rollen für zukünftige Anwendungen zu definieren, die per Fernzugriff oder über Firmware-Aktualisierungen implementiert werden. • Es MUSS möglich sein, alle implementierten Rollen aus der Ferne und einzeln zu deaktivieren.
	Empfehlung und Anleitung zur Umsetzung

	1. Der Hersteller SOLL den Nachweis erbringen, dass diese Anforderung erfüllt ist. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Diese Anforderung wird in einem funktionalen Sicherheitstest überprüft. Die Prüfung sollte insbesondere sicherstellen, dass jede Rolle nur über die definierten und notwendigen Berechtigungen verfügt.
SAR_01.GW	**Anforderung**
	Das (Hybrid-)Gateway MUSS rollenbasierte Zugriffskontrollen (Role Based Access Controls, RBAC) unterstützen, um das Gerät vor unbefugtem Zugriff zu schützen, indem unterschiedliche Zugriffsrechte auf der Grundlage der Rolle eines Benutzers durchgesetzt werden. • Das (Hybrid-)Gateway MUSS mindestens die in Abschnitt B.3.2 definierten Rollen unterstützen. • Es MUSS möglich sein, die Berechtigungen der einzelnen Rollen zu konfigurieren. • Es MUSS möglich sein, jeder Rolle individuelles Schlüsselmaterial zuzuordnen. Diese Schlüssel MÜSSEN aktualisierbar sein. • Es MUSS möglich sein, Rollen an Schnittstellen zu binden. • Es MUSS möglich sein, weitere Rollen für zukünftige Anwendungen zu definieren, die per Fernzugriff oder über Firmware-Aktualisierungen implementiert werden. • Es MUSS möglich sein, alle implementierten Rollen aus der Ferne und einzeln zu deaktivieren.
	Empfehlung und Anleitung zur Umsetzung
	1. Der Hersteller SOLL den Nachweis erbringen, dass diese Anforderung erfüllt ist. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist. 2. Wenn das Gateway Schlüssel für die Benutzerauthentifizierung verwendet (z.B. bei Verwendung von Zertifikaten in einer Webschnittstelle), muss es gemäß SFR_03.GW individuelle Schlüssel für jedes Gateway unterstützen.

	Empfohlene Qualitätssicherungsmaßnahme
	1. Diese Anforderung wird in einem funktionalen Sicherheitstest überprüft. Die Prüfung sollte insbesondere sicherstellen, dass jede Rolle nur über die definierten und notwendigen Berechtigungen verfügt.
SAR_01.CS	**Anforderung**
	Das Zentrales System MUSS rollenbasierte Zugriffskontrollen (Role Based Access Controls, RBAC) unterstützen, um vor unbefugtem Zugriff zu schützen, indem unterschiedliche Zugriffsrechte auf der Grundlage der Rolle eines Benutzers durchgesetzt werden. • Das Zentrale System MUSS mindestens die in Abschnitt B.3.3 definierten Rollen unterstützen. • Es MUSS möglich sein, die Berechtigungen der einzelnen Rollen zu konfigurieren. • Es MUSS möglich sein, jeder Rolle individuelles Schlüsselmaterial zuzuordnen. Diese Schlüssel MÜSSEN aktualisierbar sein. • Es MUSS möglich sein, Rollen an Schnittstellen zu binden. • Es MUSS möglich sein, weitere Rollen für zukünftige Anwendungen zu definieren, die per Fernzugriff oder über Software-Aktualisierungen implementiert werden. • Es MUSS möglich sein, alle implementierten Rollen einzeln zu deaktivieren. Das Zentrale System MUSS über Maßnahmen verfügen, die sicherstellen, dass autorisierte Benutzer nicht in der Lage sind, eine große Anzahl von Zählern in kurzer Zeit zu unterbrechen.
	Empfehlung und Anleitung zur Umsetzung
	1. Der Hersteller SOLL den Nachweis erbringen, dass diese Anforderung erfüllt ist. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist. 2. Die Verbindung zwischen der Benutzerautorisierung (z.B. Passwörter oder Smartcards) und den Rollen SOLL über ein geeignetes System, wie z.B. LDAP, realisiert werden. 3. Es SOLL möglich sein, Rollen einzurichten, die den Zugriff nach dem Vier-Augen-Prinzip ermöglichen.

	4. Das Zentrale System SOLL individuelle Benutzerkonten unterstützen, indem es in ein zentrales Zugangskontrollsystem, wie z.B. Active Directory, integriert wird. 5. Die Maßnahmen gegen das Schalten einer großen Anzahl von Zählern SOLLEN auch verhindern, dass die Benutzer indirekt schalten, indem sie beispielsweise Skripte auf das Zentrale System oder den Zähler aufspielen, Aktionen mit einem bestimmten Timer einstellen oder den maximalen Stromverbrauch auf Null beschränken.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Es wird empfohlen, einen Funktionstest der entsprechenden rollenbasierten Zugriffskontrollen durchzuführen. Damit soll sichergestellt werden, dass bei der Implementierung jeder Rolle nur die erforderlichen Berechtigungen erteilt wurden.
SAR_02.M	**Anforderung**
	Der Zähler MUSS Mechanismen zur Verhinderung und Erkennung von unberechtigtem Zugriff unterstützen.
	Empfehlung und Anleitung zur Umsetzung
	1. Der Zähler SOLL Mechanismen zur Erkennung unbefugter Zugriffsversuche implementieren. Wenn möglich, SOLL der Zähler den Vorfall als Sicherheitsereignis protokollieren. Ein Beispiel für ein solches Ereignis wäre der Versuch, auf ein Datenobjekt zuzugreifen, für das der Benutzer keine Berechtigung hat. 2. Der Hersteller SOLL den Nachweis erbringen, dass diese Anforderung erfüllt ist. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Die Implementierung von Erkennungsmechanismen kann in einem funktionalen Sicherheitstest überprüft werden. 2. Die Durchführung eines Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung angemessen umgesetzt wurde.

SAR_02.GW	**Anforderung**
	Das (Hybrid-)Gateway MUSS Mechanismen zur Verhinderung und Erkennung von unberechtigtem Zugriff unterstützen.
	Empfehlung und Anleitung zur Umsetzung
	1. Das (Hybrid-)Gateway SOLL Mechanismen zur Erkennung unbefugter Zugriffsversuche implementieren. Wenn möglich, SOLL das (Hybrid-)Gateway den Vorfall als Sicherheitsereignis protokollieren. Ein Beispiel für ein solches Ereignis wäre der Versuch, auf ein Datenobjekt zuzugreifen, für das der Benutzer keine Berechtigung hat. 2. Der Hersteller SOLL den Nachweis erbringen, dass diese Anforderung erfüllt ist. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Die Implementierung von Erkennungsmechanismen kann in einem funktionalen Sicherheitstest überprüft werden. 2. Die Durchführung eines Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung angemessen umgesetzt wurde.
SAR_02.CS	**Anforderung**
	Das Zentrale System MUSS Mechanismen zur Verhinderung und Erkennung von unberechtigtem Zugriff unterstützen.
	Empfehlung und Anleitung zur Umsetzung
	1. Das Zentrale System SOLL Mechanismen zur Erkennung unbefugter Zugriffsversuche implementieren. Wenn möglich, SOLL das Zentrale System den Vorfall als Sicherheitsereignis protokollieren. Ein Beispiel für ein solches Ereignis wäre der Versuch, auf ein Datenobjekt zuzugreifen, für das der Benutzer keine Berechtigung hat. 2. Der Hersteller SOLL den Nachweis erbringen, dass diese Anforderung erfüllt ist. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist.

	Empfohlene Qualitätssicherungsmaßnahme
	1. Die Implementierung von Erkennungsmechanismen kann in einem funktionalen Sicherheitstest überprüft werden. 2. Die Durchführung eines Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung angemessen umgesetzt wurde.
SAR_03.M	Anforderung
	Der Zähler MUSS sowohl erfolgreiche Anmeldungen als auch fehlgeschlagene Authentifizierungsversuche im Sicherheitsprotokoll protokollieren.
	Empfehlung und Anleitung zur Umsetzung
	1. Die Implementierung des Sicherheitsprotokolls SOLL sicherstellen, dass die Einträge keine anderen sicherheitsrelevanten Einträge überschreiben. 2. Der Zentralen System SOLL das Zentrale System nach einer konfigurierbaren Anzahl von fehlgeschlagenen Anmeldeversuchen benachrichtigen. 3. Der Hersteller SOLL den Nachweis erbringen, dass diese Anforderung erfüllt ist. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Die Implementierung einer korrekten Ereignisprotokollierung kann in einem funktionalen Sicherheitstest überprüft werden. 2. Die Durchführung eines Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung angemessen umgesetzt wurde.
SAR_03.GW	**Anforderung**
	Das (Hybrid-)Gateway MUSS sowohl erfolgreiche Anmeldungen als auch fehlgeschlagene Authentifizierungsversuche im Sicherheitsprotokoll protokollieren.
	Empfehlung und Anleitung zur Umsetzung

	1. Die Implementierung des Sicherheitsprotokolls SOLL sicherstellen, dass die Einträge keine anderen sicherheitsrelevanten Einträge überschreiben. 2. Das (Hybrid-)Gateway SOLL das Zentrale System nach einer konfigurierbaren Anzahl von fehlgeschlagenen Anmeldeversuchen benachrichtigen. 3. Der Hersteller SOLL den Nachweis erbringen, dass diese Anforderung erfüllt ist. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Die Implementierung einer korrekten Ereignisprotokollierung kann in einem funktionalen Sicherheitstest überprüft werden. 2. Die Durchführung eines Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung angemessen umgesetzt wurde.
SAR_03.CS	**Anforderung**
	Das Zentrale System MUSS sowohl erfolgreiche Anmeldungen als auch fehlgeschlagene Authentifizierungsversuche im Sicherheitsprotokoll protokollieren.
	Empfehlung und Anleitung zur Umsetzung
	1. Die Implementierung des Sicherheitsprotokolls SOLL sicherstellen, dass die Einträge keine anderen sicherheitsrelevanten Einträge überschreiben. 2. Der Hersteller SOLL den Nachweis erbringen, dass diese Anforderung erfüllt ist. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Die Implementierung einer korrekten Ereignisprotokollierung kann in einem funktionalen Sicherheitstest überprüft werden. 2. Die Durchführung eines Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung angemessen umgesetzt wurde.

C.5 Vertraulichkeit

Anf._ID	
SCR_01.M	**Anforderung**
	Die folgenden Schnittstellen des Zählers MÜSSEN die Verschlüsselung auf der Anwendungsschicht mit einem zulässigen Algorithmus unterstützen: • LAN zwischen dem Stromzähler und dem Zentralen System • WAN zwischen dem Stromzähler und dem Zentralen System • Multi-Utility-Schnittstelle zwischen dem Stromzähler und anderen Versorgungszählern • Kundenschnittstelle
	Empfehlung und Anleitung zur Umsetzung
	1. Die zulässigen Verschlüsselungsalgorithmen sind in SPR_01 definiert. 2. Die Kommunikation SOLL mit symmetrischen Algorithmen und vorzugsweise mit einer authentifizierten Chiffre verschlüsselt werden.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Diese Anforderung wird in einem funktionalen Sicherheitstest überprüft. Die Prüfung soll insbesondere sicherstellen, dass jede Schnittstelle die erlaubten Algorithmen unterstützt.
SCR_01.GW	**Anforderung**
	Die WAN-Schnittstelle und die LAN-Schnittstelle des (Hybrid-)Gateways MÜSSEN die Verschlüsselung auf der Anwendungsschicht unterstützen, mit Ausnahme der Nachrichten, die direkt zwischen dem Smart Meter und dem Zentralen System gesendet werden.
	Empfehlung und Anleitung zur Umsetzung
	1. Die zulässigen Verschlüsselungsalgorithmen sind in SPR_01 definiert. 2. Die Kommunikation SOLL mit symmetrischen Algorithmen und vorzugsweise mit einer authentifizierten Chiffre verschlüsselt werden.

	Empfohlene Qualitätssicherungsmaßnahme
	1. Diese Anforderung wird in einem funktionalen Sicherheitstest überprüft. Die Prüfung soll insbesondere sicherstellen, dass jede Schnittstelle die erlaubten Algorithmen unterstützt.
SCR_01.CS	Anforderung

	Die folgenden Schnittstellen des Zentralen Systems MÜSSEN die Verschlüsselung auf der Anwendungsschicht mit einem zulässigen Algorithmus unterstützen (wie in SPR_01 festgelegt):
	• WAN_M zwischen dem Stromzähler und dem Zentralen System
	• WAN_GW:
	  ○ zwischen dem Stromzähler und dem Zentralen System
	  ○ zwischen dem (Hybrid-)Gateway und dem Zentralen System, wenn die Schnittstelle für Wartungszwecke verwendet wird
	• Benutzeroberflächen (UI)
	• Alle internen Schnittstellen des Zentralen Systems (Zone zu Zone)
	• Web Interface (WWW) des Kundenportals
	• Schnittstelle zum Back-End-System im MDMS

	Empfehlung und Anleitung zur Umsetzung
	1. Die zulässigen Verschlüsselungsalgorithmen sind in SPR_01 definiert. 2. Die Anforderung SRR_04.CS enthält Einzelheiten zur Zoneneinteilung im Zentralen System. 3. Abschnitt B.2 enthält Einzelheiten zu den Schnittstellen des Zentralen Systems.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Diese Anforderung wird in einem funktionalen Sicherheitstest überprüft. Die Prüfung soll sicherstellen, dass jede Schnittstelle die erlaubten Algorithmen unterstützt.

C.6 Audits und Protokolle

Anf._ID	
SLR_01.M	**Anforderung**
	Der Zähler MUSS mindestens die in Abschnitt B.4 beschriebenen Sicherheitsereignisse protokollieren. Der Zähler MUSS einen lokalen Prüfpfad für alle Sicherheitsereignisse bereitstellen. Zusätzlich zu den bestehenden Protokolldateien MUSS ein spezielles Sicherheitsprotokoll vorhanden sein, um sicherheitsrelevante Ereignisse zu speichern. Das Sicherheitsprotokoll MUSS vom Zentralen System aus zugänglich sein. Der Zähler MUSS mit speziellen Registern ausgestattet sein, die die Anzahl der Sicherheitsereignisse während eines bestimmten Intervalls zählen. Dieses Intervall MUSS konfigurierbar sein.
	Empfehlung und Anleitung zur Umsetzung
	1. Jedes Sicherheitsereignis SOLL, soweit möglich, die Benutzer- oder Systemidentifikation (ID), die Schnittstelle, den Zeitstempel sowie das Ergebnis des Ereignisses aufzeichnen. 2. Der Hersteller SOLL eine Liste aller unterstützten Sicherheitsereignisse zur Verfügung stellen.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Diese Anforderung wird in einem funktionalen Sicherheitstest des Sicherheitsprotokolls überprüft. 2. Die Durchführung eines Penetrationstests wird empfohlen, um sicherzustellen, dass die Spezifikation angemessen umgesetzt wurde.
SLR_01.GW	**Anforderung**
	Das (Hybrid-)Gateway MUSS einen lokalen Prüfpfad für alle Sicherheitsereignisse bereitstellen.

	Zusätzlich zu den bestehenden Protokolldateien MUSS ein spezielles Sicherheitsprotokoll vorhanden sein, um sicherheitsrelevante Ereignisse zu speichern. Das Sicherheitsprotokoll MUSS vom Zentralen System aus zugänglich sein. Das (Hybrid-)Gateway MUSS mindestens die in Abschnitt B.4 beschriebenen Sicherheitsereignisse protokollieren.
	Empfehlung und Anleitung zur Umsetzung
	1. Jedes Sicherheitsereignis SOLL, soweit möglich, die Benutzer- oder Systemidentifikation (ID), die Schnittstelle, den Zeitstempel sowie das Ergebnis des Ereignisses aufzeichnen. 2. Der Hersteller SOLL eine Liste aller unterstützten Sicherheitsereignisse zur Verfügung stellen.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Diese Anforderung wird in einem funktionalen Sicherheitstest des Sicherheitsprotokolls überprüft. 2. Die Durchführung eines Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung angemessen umgesetzt wurde.
SLR_01.CS	**Anforderung**
	Das Zentrale System MUSS einen lokalen Prüfpfad für alle Sicherheitsereignisse bereitstellen. Zusätzlich zu den bestehenden Protokolldateien MUSS ein spezielles Sicherheitsprotokoll vorhanden sein, um sicherheitsrelevante Ereignisse zu speichern, oder es MUSS möglich sein, eine Protokolldatei nach allen sicherheitsrelevanten Ereignissen zu filtern.
	Empfehlung und Anleitung zur Umsetzung
	1. Jedes Sicherheitsereignis SOLL, soweit möglich, die Benutzer- oder Systemidentifikation (ID), die Schnittstelle, den Zeitstempel sowie das Ergebnis des Ereignisses aufzeichnen. 2. Der Hersteller SOLL eine Liste aller unterstützten Sicherheitsereignisse zur Verfügung stellen.

	3. Das Zentrale System SOLL die Sicherheitsereignisse an ein Protokollüberwachungs- oder SIEM-System weiterleiten, um die Überwachung und Analyse durch ein Security Operations Center zu ermöglichen.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Diese Anforderung wird in einem funktionalen Sicherheitstest des Sicherheitsprotokolls überprüft. 2. Die Durchführung eines Penetrationstests wird empfohlen, um sicherzustellen, dass die Spezifikation angemessen umgesetzt wurde.
SLR_02	**Anforderung**
	Die Einträge aller Protokolldateien MÜSSEN vor Änderungen geschützt werden, nur das Hinzufügen neuer Einträge darf möglich sein.
	Empfehlung und Anleitung zur Umsetzung
	1. Rollenbasierte Zugriffskontrollen SOLLEN das Sicherheitsprotokoll schützen.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Die Durchführung eines Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung angemessen umgesetzt wurde.
SLR_03.M	**Anforderung**
	Der Zähler MUSS genügend Speicher für das Sicherheitsprotokoll bereitstellen, um mindestens die letzten 100 Sicherheitsereignisse zu speichern. Die Sicherheitsprotokolldatei MUSS als rollierende Protokolldatei eingerichtet werden.
	Empfehlung und Anleitung zur Umsetzung

	1. Der Hersteller SOLL den Nachweis erbringen, dass diese Anforderung erfüllt ist. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Die Anforderung wird durch einen Funktionstest überprüft, um sicherzustellen, dass das Sicherheitsprotokoll über eine ausreichende Kapazität verfügt.
SLR_03.GW	**Anforderung**
	Das (Hybrid-)Gateway MUSS genügend Speicher für das Sicherheitsprotokoll bereitstellen, um mindestens die letzten 1000 Sicherheitsereignisse zu speichern. Die Sicherheitsprotokolldatei MUSS als rollierende Protokolldatei eingerichtet werden.
	Empfehlung und Anleitung zur Umsetzung
	1. Der Hersteller SOLL den Nachweis erbringen, dass diese Anforderung erfüllt ist. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Die Anforderung wird durch einen Funktionstest überprüft, um sicherzustellen, dass das Sicherheitsprotokoll über eine ausreichende Kapazität verfügt.
SLR_03.CS	**Anforderung**
	Die Komponenten des Zentralen Systems MÜSSEN eine Verbindung zu einem Protokollierungsserver unterstützen. Es MUSS möglich sein, den Protokollserver auf einem eigenen System zu betreiben (d.h. nicht auf dem HES, MDMS oder KMS).

	Empfehlung und Anleitung zur Umsetzung
	1. Das Zentrale System SOLL einen eigenen Protokollierungsserver (z.B. einen Syslog-Server) unterstützen. Dieser Protokollserver SOLL alle Sicherheitsereignisse aller Komponenten des Zentralen Systems protokollieren. 2. Der Hersteller SOLL den Nachweis erbringen, dass diese Anforderung erfüllt ist. Der Nachweis SOLL so detailliert sein, dass eine einfache Überprüfung möglich ist.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Die Anforderung wird durch einen Funktionstest überprüft, um sicherzustellen, dass der Protokollserver die Sicherheitsereignisse korrekt verwaltet.

C.7 Produktlebenszyklus und Governance

Anf._ID	
SDR_01	**Anforderung**
	Der Hersteller MUSS eine ISO/IEC 27001-Zertifizierung für alle Entwicklungs-, Herstellungs- und Bereitstellungsprozesse für Geräte und Produkte vorweisen können, die im Smart-Metering-System (Zähler, Gateways und Anwendungen des Zentralen Systems) eingesetzt werden. Der Nachweis der Zertifizierung muss spätestens bei der Lieferung erbracht werden.
	Empfehlung und Anleitung zur Umsetzung
	1. Die Anforderung gilt für alle sicherheitsrelevanten Entwicklungsprozesse, Herstellungsprozesse und Bereitstellungsprozesse für den Zähler und das (Hybrid-)Gateway. 2. Die Anforderung gilt für alle sicherheitsrelevanten Entwicklungsprozesse, Herstellungsprozesse und Bereitstellungsprozesse für den Zähler und das (Hybrid-)Gateway. 3. Werden sicherheitsrelevante Komponenten von Drittanbietern bezogen, so MÜSSEN die entsprechenden Bereiche und Übergabeprozesse nach ISO/IEC 27001 zertifiziert sein.

	4. Darüber hinaus SOLL die Norm ISO/IEC 27001 auf alle sicherheitsrelevanten Werkzeuge und Geräte angewandt werden, die in der Smart-Metering-Architektur verwendet werden, z.B. das Handbediengerät oder die Wartungssoftware. 5. Der Hersteller SOLL die Sicherheitsrichtlinien des Unternehmens teilen.
SDR_02	**Anforderung**
	Der Hersteller MUSS für die Verwaltung der Produkte ein sicheres Konfigurationsmanagementsystem verwenden. Alle Änderungen der hinterlegten Informationen MÜSSEN angemessen, nachvollziehbar, geprüft und dokumentiert sein. 1. Der Hersteller MUSS angemessene Maßnahmen ergreifen, um die IT-Sicherheit und die physische Sicherheit des Konfigurationsmanagementsystems zu gewährleisten. 2. Der Hersteller MUSS einen Audit-Mechanismus bereitstellen, der den Benutzer jeder vorgenommenen Änderung identifiziert. 3. Drittanbieter von sicherheitsrelevanten Funktionen und Produkten MÜSSEN vergleichbare Prozesse für das Konfigurationsmanagement implementieren.
	Empfehlung und Anleitung zur Umsetzung
	1. Die Anforderung gilt insbesondere für die Entwicklungsprozesse, die Herstellungsprozesse und die Bereitstellungsprozesse für Zähler, (Hybrid-)Gateway und Zentrales System. 2. Die folgenden Beispiele für ein sicheres Konfigurationsmanagementsystem SOLLEN berücksichtigt werden: • Verwaltung von Hardwarekonfigurationen von Geräten und deren Änderungen. • Verwaltung von Quellcode und Firmware und deren Änderungen. • Verwaltung von (kundenbezogenen) Parametern von Geräten und deren Änderungen.
SDR_03	**Anforderung**
	Gesicherter Versionierungsprozess: 1. Alle freigegebenen Versionen (Hardware und Firmware) eines Geräts oder Produkts MÜSSEN eindeutig identifizierbar sein.

	2. Jeder Version MUSS eine allen Beteiligten zugängliche Release-Note beiliegen, in der die vorgenommenen Änderungen aufgeführt sind. 3. Die Firmware MUSS durch ihren Hash-Wert eindeutig identifizierbar sein. 4. Der Hersteller MUSS in der Lage sein, freigegebene Versionen für Geräte innerhalb des Produktlebenszyklus zu reproduzieren, wobei die Rückverfolgbarkeit durch den/die Hash-Wert(e) als Identifikator(en) gewährleistet wird. 5. Auswechselbare Hardwaremodule MÜSSEN separat versioniert werden. 6. Software und Software-Aktualisierungen MÜSSEN durch ihren Hash-Wert eindeutig identifizierbar sein.
	Empfehlung und Anleitung zur Umsetzung
	1. Die Anforderung betrifft die Versionierungsprozesse für die Entwicklung der Firmware des Zählers und des (Hybrid-)Gateways. 2. Außerdem betrifft die Anforderung die Versionierungsprozesse für die Entwicklung von Software, die im Zentralen System verwendet wird. 3. In der Anforderung SPR_01 sind die zulässigen kryptografischen Hash-Algorithmen aufgeführt. 4. In Anhang A.2 wird ein Beispielprozess für die Erstellung digitaler Signaturen beschrieben.
SDR_04	**Anforderung**
	Der Hersteller MUSS ein Fehlerbehebungs- und Meldeverfahren einführen: 1. Der Hersteller MUSS aktiv auf Schwachstellen achten und sich aktiv an der Prüfung auf Schwachstellen beteiligen. Der Hersteller MUSS unverzüglich Informationen über Schwachstellen zur Verfügung stellen und umgehend Aktualisierungen zur Behebung von Schwachstellen bereitstellen, die alle technischen Möglichkeiten berücksichtigen. 2. Die Hersteller MÜSSEN ein Verfahren für extern gemeldete Schwachstellen einführen.
	Empfehlung und Anleitung zur Umsetzung
	1. Die Anforderung betrifft die Fehlerbehebungs- und Meldeverfahren für die Entwicklung und Herstellung des Zählers, des (Hybrid-)Gateways und des Zentralen Systems.

	2. Die folgenden Fälle eines Fehlerbehebungs- und Meldeverfahrens SOLLEN in Betracht gezogen werden: • Identifizierung und Behebung der vom Hersteller festgestellten Sicherheitsmängel. • Identifizierung und Behebung der vom Netzbetreiber festgestellten Sicherheitsmängel. • Identifizierung und Behebung von Sicherheitsmängeln, die von externen Parteien gefunden wurden, z.B. von Forschern veröffentlichte Sicherheitsmängel. 3. Zwischen dem Hersteller und dem Betreiber SOLL eine Dienstgütevereinbarung (SLA) über die Meldung und Behebung von Schwachstellen getroffen werden. Es SOLL ein Zeitplan für die Behebung von Schwachstellen auf der Grundlage ihres Schweregrads, z.B. durch ihren CVSS-Score, festgelegt werden.
SDR_05	**Anforderung**
	Der Hersteller MUSS die Produkte umfassend prüfen. Diese Prüfungen MÜSSEN Sicherheitstests umfassen, einschließlich Prüfungen der kryptografischen Maßnahmen. 1. Alle Geräte MÜSSEN mit den Spezifikationen der vom Hersteller gelieferten Dokumentation übereinstimmen. 2. Mit Hilfe von nicht-trivialen Prüffällen MUSS der Hersteller in der Lage sein, den Nachweis des korrekten Verhaltens bei Sicherheits- und Funktionstests zu erbringen. 3. Die Prüfungen MÜSSEN den gesamten Funktionsumfang des Produkts abdecken und insbesondere Prüfungen der gesamten Kommunikationskette umfassen. 4. Die Prüfungen MÜSSEN sowohl regelmäßig genutzte als auch selten genutzte Funktionen, wie z.B. Software-Aktualisierungen, angemessen testen. 5. Der Hersteller MUSS dem Netzbetreiber die Ergebnisse der durchgeführten Sicherheitstests zum Zeitpunkt der Freigabe zur Verfügung stellen. 6. Der Hersteller MUSS nach größeren Änderungen neue Funktionen testen und mindestens alle drei Jahre Prüfungen durchführen, die den gesamten Funktionsumfang abdecken. 7. Der Hersteller MUSS die Prüfung durch einen unabhängigen Dritten auf Anfrage des Betreibers unterstützen, indem er die erforderlichen Unterlagen, den Zugang und die technische Unterstützung bereitstellt.

	Der Hersteller MUSS es einer unabhängigen dritten Partei ermöglichen, Quellcodeüberprüfungen durchzuführen.
	Empfehlung und Anleitung zur Umsetzung
	1. Die Anforderung betrifft die Sicherheitsprüfung des Zählers, des (Hybrid-)Gateways und des Zentralen Systems. 2. Die folgenden Beispiele für Sicherheitstests SOLLEN berücksichtigt werden: • Fuzzing-Tests • Robustheitstests • Penetrationstests In Anhang B sind Einzelheiten zu den oben genannten Prüfarten aufgeführt. 3. Die Überprüfung des Quellcodes kann zum Schutz des Quellcodes vor Ort beim Hersteller durchgeführt werden.
SDR_06	**Anforderung**
	Der Hersteller MUSS über ein hohes IKT-Sicherheitsbewusstsein verfügen und das Personal in Sachen IKT-Sicherheit schulen. Der Hersteller MUSS nachweisen, dass er über die erforderlichen Kenntnisse zur Entwicklung und Herstellung sicherer Produkte verfügt. Der Hersteller MUSS einen technischen Ansprechpartner für sicherheitsrelevante Fragen benennen.
	Empfehlung und Anleitung zur Umsetzung
	1. Beispiel: • Nachgewiesene Berufserfahrung auf dem Gebiet der IT-Sicherheit oder eine Sicherheitszertifizierung wie CISSP oder CISM.
SDR_07	**Anforderung**
	Sicherheitssteigernde Merkmale der zugrunde liegenden Plattform, Implementierungssprache und Werkzeugkette MÜSSEN eingesetzt werden. Der Hersteller MUSS einen Nachweis erbringen, falls dies nicht notwendig oder möglich ist.

	Empfehlung und Anleitung zur Umsetzung
	1. Beispiele für sicherheitserhöhende Merkmale sind: • Sicherer Bootvorgang, bei dem der Bootloader die Authentizität der Firmware prüft. • Deaktivierung von Hardware-Debug-Schnittstellen, wie z.B. JTAG-Schnittstellen. • Aktivierung der Funktionen des Mikrocontrollers, die den Ausleseschutz ermöglichen.
SDR_08	**Anforderung**
	Der Hersteller MUSS die sichere Bereitstellung der kryptografischen Schlüssel während des Herstellungsprozesses gewährleisten. Es MUSS möglich sein, jedes kryptografische Schlüsselmaterial den Geräten im Rahmen des Herstellungsprozesses individuell zur Verfügung zu stellen. Der Hersteller MUSS einen sicheren Übergabeprozess an den Netzbetreiber gewährleisten.
	Empfehlung und Anleitung zur Umsetzung
	1. Beispiele: • Der Hersteller SOLL einen gesicherten Produktionsbereich zur Verfügung stellen, um die sichere Erstbereitstellung der kryptografischen Schlüssel zu gewährleisten. • Es SOLL ein sicheres Verfahren zur Übergabe der bereitgestellten Informationen an das Zentrale System eingerichtet werden. • In Anhang A.1 wird ein Beispielprozess für eine gesicherte Bereitstellung beschrieben.
SDR_09	**Anforderung**
	Der Hersteller MUSS ein Sicherheitskonzept und eine detaillierte Dokumentation der Komponenten des Zentralen Systems vorlegen, die einem Dritten eine Fernwartungsfunktion bieten.
	Empfehlung und Anleitung zur Umsetzung

	1. Fernwartungsfunktionen SOLLEN nach Möglichkeit vermieden werden. 2. Ein Beispiel für die Absicherung der Fernwartungsfunktion wäre ein Terminalserver.
SDR_10	**Anforderung**
	Das Zentrale System MUSS ein Verfahren zur sicheren Entsorgung von Zählern und (Hybrid-)Gateways unterstützen, indem es diese im System deaktiviert und die kryptografischen Schlüssel außer Betrieb nimmt.
	Empfehlung und Anleitung zur Umsetzung
	1. Siehe Anhang A.5 für Empfehlungen zum Entsorgungsprozess.

C.8 Sicherheitselement

Die folgenden Anforderungen betreffen das Sicherheitselement eines Hybrid-Gateways. *Diese Anforderungen gelten nur für den Fall, dass eine hybride Architektur verwendet wird* (Option C in Abschnitt B.1). Sie gelten nicht für Option B und Nicht-Hybrid-Gateways.

Anf._ID	
SER_01.GW	**Anforderung**
	Das Hybrid-Gateway MUSS über ein Sicherheitselement zum Schutz aller gespeicherten Schlüssel verfügen. Das Sicherheitselement MUSS die folgenden Anforderungen erfüllen: • Das Sicherheitselement erhält die Schlüssel vom HSM im Zentralen System, so dass die Integrität und Vertraulichkeit durchgehend geschützt sind. • Gespeicherte Schlüssel sind gegen fortgeschrittene physische Bedrohungen geschützt, bei denen Angreifer vollen physischen Zugriff auf das Gerät haben. • Die Kommunikation zwischen dem Hauptprozessor und dem Sicherheitselement ist kryptografisch geschützt, um Man-in-the-Middle-Angriffe zu verhindern. Das Sicherheitselement muss nach Common Criteria (CC) anhand von Sicherheitsvorgaben zertifiziert sein, die die obigen Anforderungen abdecken

	und eine Vertrauenswürdigkeitsstufe von EAL 4 oder höher aufweisen. Der Verkäufer muss alle einschlägigen Common-Criteria-Zertifikate vorlegen.
	Empfehlung und Anleitung zur Umsetzung
	1. Für den IC, die Plattform und das Applet können separate Common-Criteria-Zertifikate vorgelegt werden. 2. Das Sicherheitselement schützt alle vom Hybrid-Gateway verwendeten Schlüssel, einschließlich derer für die Kommunikation mit den Zählern, sowie alle privaten Schlüssel, die für TLS oder SSH verwendet werden. 3. Die im Sicherheitselement verwendeten kryptografischen Algorithmen müssen den Anforderungen in Abschnitt C.1.3 entsprechen.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Die Anforderungen werden durch Einsichtnahme in das Zertifikat des Sicherheitselements überprüft. Die Sicherheitsvorgaben, nach denen das Element zertifiziert wird, müssen die richtige Sicherheitsstufe haben und die aufgeführten Anforderungen abdecken. 2. Es wird empfohlen, eine Codeüberprüfung durchzuführen, um festzustellen, wie das Sicherheitselement von den Anwendungen auf dem Datenkonzentrator korrekt verwendet wird.
SER_02.GW	**Anforderung**
	Das Hybrid-Gateway MUSS über Hardware-Unterstützung für sicheres Booten verfügen, bei dem die Authentizität der gesamten während der Boot-Sequenz geladenen Software kryptografisch überprüft wird. Der sichere Bootvorgang: • hat eine Vertrauensbasis, die in unveränderlicher Hardware (ROM oder OTP) verankert ist • schützt die Vertraulichkeit und Integrität aller Teile der sicheren Boot-Kette • überprüft die Authentizität aller Daten vor der Verwendung kryptografisch • kopiert alle Daten vor der Überprüfung und Entschlüsselung in den flüchtigen Speicher (SRAM/DRAM)

	Empfehlung und Anleitung zur Umsetzung
	Idealerweise sollte auch eine Anti-Rollback-Funktion implementiert werden, damit ein Angreifer die Firmware nicht auf eine bekannte verwundbare Version downgraden kann. Dies kann jedoch zu betrieblichen Problemen führen, wenn die neu eingeführte Firmware-Version Probleme aufweist. Eine Lösung für dieses Problem besteht darin, dass der Hersteller auch die vorherige Version der Firmware so signiert, als ob es sich um die nächste Version handeln würde. Ein solches System würde jedoch auch vorschreiben, dass die Firmware die Kunden-ID enthalten muss, damit andere Kunden nicht mit diesem Downgrade angegriffen werden können.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Die Anforderungen werden überprüft, indem ein Zertifikat angefordert wird, aus dem hervorgeht, dass die Hardware in der Lage ist, sicheres Booten zu unterstützen. 2. Es wird empfohlen, einen Penetrationstest durchzuführen, um zu überprüfen, ob die Firmware des Gateways den sicheren Bootvorgang korrekt ausführt.
SER_03.GW	**Anforderung**
	Das Hybrid-Gateway muss in der Lage sein, die Integrität und Vertraulichkeit aller Daten, die nicht auf demselben Paket wie der Prozessor gespeichert sind, kryptografisch zu schützen. Die verwendeten Schlüssel werden in Hardware gespeichert, die gegen fortgeschrittene physische Angriffe resistent ist. Vor jeder Verwendung prüft der Prozessor, ob die aus dem Speicher geladenen Daten seit dem Schreiben nicht verändert wurden.
	Empfehlung und Anleitung zur Umsetzung
	-
	Empfohlene Qualitätssicherungsmaßnahme
	1. Es wird empfohlen, einen Penetrationstest durchzuführen, um zu überprüfen, ob die gespeicherten Daten wie erforderlich geschützt sind.

SER_04.GW	**Anforderung**
	Das Hybrid-Gateway DARF nur Zugriff auf die Schlüssel für die Hybrid-Gateway-Rolle haben, wie in Abschnitt B.3.1 beschrieben.
	Empfehlung und Anleitung zur Umsetzung
	1. Das Hybrid-Gateway hat keinen Zugriff auf die anderen Schlüssel, z.B. die für das Zentrale System, um zu verhindern, dass es kritische Befehle ausführt.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Es wird empfohlen, einen Penetrationstest durchzuführen, um zu überprüfen, ob die gespeicherten Daten wie erforderlich geschützt sind.

Anhang A Beispiel-Prozesse

Die beschriebenen Prozesse sind Beispiele dafür, wie ausgewählte Anforderungen im Rahmen der Ende-zu-Ende-Sicherheit umgesetzt werden können. Die folgenden Abschnitte mit Beispielprozessen sind nicht normativ, sondern sollen als Verständnishilfe verstanden werden.

Anhang A.1 Verfahren für die Bereitstellung von kryptografischem Schlüsselmaterial

Eine der wichtigsten Anforderungen an die Sicherheitsarchitektur des Smart-Metering-Systems ist die Verwendung von kryptografischem Schlüsselmaterial, das pro Gerät und pro auf dem Gerät konfigurierter Rolle eindeutig sein muss. Das kryptografische Schlüsselmaterial muss kryptografisch sicher nach dem Zufallsprinzip erzeugt und sicher für das Gerät bereitgestellt und gespeichert werden.

Um den Installationsprozess zu optimieren und gleichzeitig die Sicherheit zu gewährleisten, wird empfohlen, die Bereitstellung des Schlüsselmaterials beim Hersteller als einen der letzten Schritte im Herstellungsprozess durchzuführen. Dieses anfängliche kryptografische Schlüsselmaterial wird verwendet, um eine erste, sichere Verbindung mit den Geräten herzustellen, z.B. vom Zentralen System oder vom Handbediengerät aus. Die Sicherheit der Kommunikation zwischen diesen Geräten beruht daher auf den beim Hersteller etablierten Verfahren zur Bereitstellung des kryptografischen Schlüsselmaterials.

Daraus ergeben sich die folgenden Hauptpunkte, die zu berücksichtigen sind:

- Anforderungen an die Vertrauenswürdigkeit der Prozessumgebung
- Prozessanforderungen für die Erzeugung und Bereitstellung des kryptografischen Schlüsselmaterials
- Anforderungen an die Übertragungsprozesse des bereitgestellten kryptographischen Schlüsselmaterials

Die Bereiche, die in den Geltungsbereich des Herstellers fallen, müssen gemäß der Anforderung SDR_01 nach ISO/IEC27001 zertifiziert sein.

Anhang A.1.1 Anforderungen an die Prozessumgebung

Die Prozessumgebung selbst muss mehrere Anforderungen erfüllen, um die Vertrauenswürdigkeit des bereitgestellten kryptografischen Schlüsselmaterials zu gewährleisten.

Erstens muss die Vertrauenswürdigkeit der Hardware, die mit kryptografischem Schlüsselmaterial ausgestattet werden soll, vom Hersteller garantiert werden. Der Hersteller muss nachweisen, dass keine Manipulationen an der Hardware vorgenommen wurden.

Außerdem muss die Vertrauenswürdigkeit der Firmware auf dem Gerät gewährleistet sein. Der Hersteller muss in der Lage sein, die Authentizität der Firmware des bereitzustellenden Geräts zu beweisen.

Als dritter Punkt muss die Sicherheit des Bereitstellungsraums selbst gewährleistet sein. Dazu gehören insbesondere die Sicherheit der verwendeten IT-Komponenten und die physischen Zugangskontrollen des Bereitstellungsbereichs.

Anhang A.1.2 Anforderungen an die Erzeugung und Bereitstellung

Die Erzeugung, Bereitstellung und Speicherung von kryptografischem Schlüsselmaterial muss in einer sicheren Prozessumgebung erfolgen.

Zur Erzeugung des kryptografischen Schlüsselmaterials ist ein zugelassener Zufallszahlengenerator zu verwenden, wie in der Anforderung SPR_02 beschrieben.

Es muss unterschieden werden, ob ein symmetrischer Schlüssel oder ein öffentliches/privates Schlüsselpaar verwendet werden soll:

- Die anfänglichen symmetrischen Schlüssel sollen außerhalb des Geräts, innerhalb der sicheren Prozessumgebung, mit einem externen Zufallszahlengenerator erzeugt werden. Der auf diese Weise erzeugte Schlüssel wird dann dem Gerät zur Verfügung gestellt.
- Ein öffentliches/privates Schlüsselpaar wird innerhalb des Geräts und innerhalb der sicheren Prozessumgebung erzeugt. Teile der Entropie für die Erzeugung des privaten Schlüssels sollten durch einen externen Zufallszahlengenerator erzeugt werden. Für das Gerät sollte ein entsprechender Zufallswert bereitgestellt werden. Nach der Erzeugung des Schlüsselpaares darf es nur möglich sein, den öffentlichen Schlüssel in Form eines Certificate Signing Requests (CSRs) vom Gerät zu erhalten. Nach der Verarbeitung der CSRs zu einem gültigen Gerätezertifikat muss dieses zusammen mit anderen Informationen (z.B. Stammzertifikaten) sicher in das Gerät importiert werden.
- Jedes von den Geräten verwendete Schlüsselmaterial sollte im Rahmen des Bereitstellungsprozesses beim Hersteller individuell initialisiert werden.

Anhang A.1.3 Anforderungen an den Transferprozess

Der Hersteller und der Betreiber des Zentralen Systems müssen gemeinsam sichere Verfahren für den Austausch des bereitgestellten kryptografischen Schlüsselmaterials anwenden. Die Vertraulichkeit und Authentizität des bereitgestellten kryptografischen Schlüsselmaterials muss bei der Übertragung gewährleistet sein.

Ein solcher Übertragungsprozess kann z.B. mit Hilfe von Verschlüsselungsmechanismen und digitalen Signaturen modelliert werden:

Hersteller und Betreiber des Zentralen Systems können jeweils ein öffentliches/privates Schlüsselpaar erzeugen und ihre öffentlichen Schlüssel auf sichere Weise, d.h. über eine Public-Key-Infrastruktur (PKI), austauschen.

Die Authentizität der ausgetauschten öffentlichen Schlüssel muss streng überprüft und dokumentiert werden.

Der Hersteller verwendet nun den erhaltenen öffentlichen Schlüssel, um alle bereitgestellten sensiblen Daten der Geräte zu verschlüsseln (z.B. alle Schlüssel, die individuell für jede Rolle auf einem Gerät generiert werden).

Diese verschlüsselten Daten werden vom Hersteller in eine elektronische Versanddatei oder ein gleichwertiges Dokument eingefügt, das vom Betreiber des Zentralen Systems verarbeitet werden kann. Der VDE Elektronische Lieferschein[5] bietet ein Standardformat für eine Versanddatei, das nützlich sein kann.

Die Seriennummer (oder eine andere eindeutige Gerätekennung) eines Geräts wird den verschlüsselten Informationen zugeordnet. Bevor diese elektronische Versanddatei dem Betreiber des Zentralen Systems zur Verfügung gestellt wird, signiert der Hersteller die Datei mit seinem eigenen privaten Schlüssel.

Beim Empfang prüft der Betreiber des Zentralen Systems die digitale Signatur des Herstellers der elektronischen Sendungsdatei mit Hilfe des öffentlichen Schlüssels des Herstellers und verifiziert so die Echtheit des empfangenen Dokuments.

In einem zweiten Schritt kann der Betreiber des Zentralen Systems die vom Hersteller verschlüsselten Informationen entschlüsseln und die Daten in das Zentrale System importieren. Unverschlüsselte Daten sollten nicht gespeichert werden und MÜSSEN anschließend sicher entfernt werden.

Für die Sicherung des Zugriffs auf den jeweiligen privaten Schlüssel gelten ähnliche Anforderungen wie in "Firmware-Aktualisierungsprozess" beschrieben.

Anhang A.2 Firmware-Aktualisierungsprozess

Die Integrität der Firmware wird durch das Anbringen einer digitalen Signatur sichergestellt. Anhand der digitalen Signatur kann das Gerät überprüfen, ob die Firmware vom Hersteller stammt. Das Gerät darf die Firmware nur akzeptieren, wenn es die Urheberschaft des Herstellers anhand der digitalen Signatur eindeutig nachweisen kann.

Um die Vertrauenswürdigkeit einer digitalen Signatur zu gewährleisten, muss der Hersteller ein Verfahren zur sicheren Erzeugung digitaler Signaturen einrichten.

[5] https://www.vde.com/de/fnn/arbeitsgebiete/digitalisierung-metering/vorbereitungen-rollout/hinweis-e-lieferschein

Anhang A.2.1 Hintergrund Digitale Signaturen

Bei der Erstellung einer digitalen Signatur wird zunächst ein Hash-Wert der Datei berechnet. Die digitale Signatur ist das Ergebnis der Verschlüsselung des Hash-Wertes mit dem privaten Schlüssel des Herstellers. Beim Empfang der Firmware prüft das Gerät die digitale Signatur mit dem öffentlichen Schlüssel und vergleicht dann den Hash-Wert der empfangenen Datei.

Daraus ergeben sich die folgenden Hauptpunkte, die zu berücksichtigen sind:

- Anforderungen an den Freigabeprozess für Firmware-Aktualisierungen.
- Anforderungen an die Zugriffsverfahren und die Sicherheit des geheimen kryptografischen Schlüsselmaterials, mit dem die digitale Signatur der Firmware-Datei erstellt wird (siehe Anforderungen an die Schlüsselverwaltung).
- Anforderungen an den Prozess der sicheren Bereitstellung von öffentlichem kryptografischem Schlüsselmaterial auf dem Gerät (siehe Anforderung SDR_07).
- Anforderungen an den Aktualisierungsprozess des Geräts selbst (siehe Anforderungen SIR_03. *).

Es wird dringend empfohlen, dass die beschriebenen Bereiche nach ISO27001 zertifiziert sind (siehe Anforderung SDR_01).

In diesem Abschnitt werden geeignete Beispielprozesse und relevante Anforderungen in Bezug auf die IKT-Sicherheit beschrieben.

Anhang A.2.2 Firmware-Release-Prozess

Der Hersteller soll ein Freigabeverfahren für neue Firmware-Versionen einrichten. Der Hersteller soll eine Person benennen, die für das Zulassungsverfahren verantwortlich ist.

Der Freigabeprozess soll vom Hersteller dokumentiert werden. Der Prozess muss relevante Nachweise für den Freigabeprozess von Firmware-Versionen liefern. Es ist wichtig zu wissen, welche Person zu welchem Zeitpunkt die Freigabe von Firmware-Aktualisierungen genehmigt hat.

Die Version der Firmware-Aktualisierungen muss anhand ihres Hash-Wertes dokumentiert werden. Besteht eine Firmware-Aktualisierung aus mehreren Komponenten (d.h. verschiedenen Dateien), müssen diese einzeln benannt und anhand ihres Hash-Werts dokumentiert werden. Mit der Freigabe einer Firmware-Aktualisierung dokumentiert der Hersteller, dass die Firmware-Datei anhand ihres Hash-Wertes eindeutig identifiziert werden kann.

Anhang A.2.3 Verwaltung und Sicherung von geheimem Schlüsselmaterial

Nach einer Firmware-Freigabe muss eine digitale Signatur erstellt werden. Besteht eine Firmware-Aktualisierung aus mehreren Komponenten (d.h. verschiedenen Dateien), müssen diese einzeln signiert werden.

Der Hersteller muss ein System betreiben, das den Zugriff auf das geheime Schlüsselmaterial kontrolliert, das für die Signaturerstellung von Firmware-Aktualisierungen verwendet wird.

Dieses System muss in einer sicheren IT-Umgebung betrieben werden.

Der Hersteller soll eine Person benennen, die für die Erstellung von digitalen Signaturen verantwortlich ist. Diese Person muss dann das System nutzen, um eine digitale Signatur für die Firmware zu erstellen. Es kann sinnvoll sein, das Vier-Augen-Prinzip auf das Signieren von Firmware anzuwenden.

Es darf nicht möglich sein, dass die verantwortliche Person direkten Zugang zu den Signierschlüsseln hat. Das System darf nur Funktionen anbieten, die die Firmware digital signieren. Darüber hinaus muss das System einen Audit-Mechanismus bereitstellen, der bei der Erstellung einer Signatur den Zeitpunkt, die verantwortliche Person, die Firmware-Version und den Hashwert der Firmware nachweist.

Darüber hinaus muss das System das geheime Schlüsselmaterial ausreichend gegen physischen Zugriff schützen, beispielsweise durch Speicherung des Schlüssels auf einem Hardware-Sicherheitsmodul.

Nach erfolgreicher Erstellung der Signatur kann die freigegebene Firmware-Version zusammen mit der Signatur zur endgültigen Firmware-Aktualisierung kombiniert werden. Diese Firmware-Aktualisierung wird dem Betreiber des Zentralen Systems zur Verfügung gestellt.

Anhang A.2.4 Bereitstellungsprozess

Damit die digitale Signatur einer Firmware-Aktualisierung automatisch überprüft werden kann, muss das entsprechende öffentliche Schlüsselmaterial auf dem Gerät bereitgestellt werden.

Dieser Bereitstellungsprozess des öffentlichen Schlüsselmaterials muss zunächst beim Hersteller in einer sicheren Umgebung durchgeführt werden. Dieses Verfahren gewährleistet die Authentizität des öffentlichen Schlüsselmaterials, das auf dem Gerät bereitgestellt wird.

Das öffentliche Schlüsselmaterial kann anschließend durch eine autorisierte (digital signierte) Firmware-Aktualisierung geändert werden.

Im Idealfall wird dieser Bereitstellungsprozess zusammen mit der Bereitstellung aller erforderlichen kryptografischen Schlüssel durchgeführt.

Anhang A.2.5 Aktualisierungsprozess des Geräts

Bevor ein Gerät eine Firmware-Datei zur Aktualisierung akzeptieren kann, muss es die digitale Signatur der Datei überprüfen. Schlägt die Überprüfung fehl oder fehlt eine digitale Signatur ganz, darf das Gerät die Firmware nicht akzeptieren. So kann das Gerät sicherstellen, dass die empfangene Firmware-Aktualisierung authentisch ist, d.h. tatsächlich vom Hersteller stammt.

Anhang A.3 Firmware-Aktualisierungsprozess

Multicast ist eine nützliche Methode, um Firmware-Aktualisierungen, die viel Bandbreite benötigen, an mehrere Geräte gleichzeitig zu senden. Nach der IMA-VO müssen bei der Verwendung von Multicast die entsprechenden Daten verschlüsselt und authentifiziert werden. Daher wird der Multicast-Prozess durch einzelne Unicasts eingeleitet.

Daraus ergibt sich der folgende Beispielprozess:

1. Das Zentrale System erstellt einen temporären Multicast-Schlüssel. Dieser Multicast-Schlüssel ist für alle Geräte gleich, muss aber mit dem individuellen Schlüssel des Geräts verschlüsselt und authentifiziert werden und kann dann per Unicast an das entsprechende Gerät gesendet werden.
2. Das Zentrale System sendet die Firmware-Aktualisierung per Multicast an alle initialisierten Geräte. Die Firmware-Aktualisierung wird verschlüsselt und mit dem zuvor generierten Multicast-Schlüssel authentifiziert. Dann verwirft das Zentrale System den Multicast-Schlüssel.
3. Das Zentrale System sendet eine Aktivierungsnachricht per Unicast an alle initialisierten Geräte. Jede Aktivierungsnachricht wird verschlüsselt und mit dem individuellen Schlüssel des Geräts authentifiziert.
4. Das Gerät entschlüsselt und prüft die Integrität der Nachricht, die die Firmware-Aktualisierung enthält. Dann verwirft das Gerät den Multicast-Schlüssel.
5. Anschließend prüft das Gerät die Integrität der Firmware-Datei anhand der digitalen Signatur und der Gültigkeit der Versionsnummer (siehe auch Anhang A.2).
6. Das Gerät aktiviert die Firmware, nachdem es die Aktivierungsnachricht erhalten, sie entschlüsselt und die Integrität überprüft hat.

Anhang A.4 Gesicherter Eich- oder Verifizierungsprozess

Die folgende Prozessbeschreibung ist ein Beispiel für die Gewährleistung der Sicherheit des Zählers, wenn es einen Eich- oder Prüfprozess durchläuft. Dieser Beispielprozess kann sowohl für unternehmensinterne Eich- oder Prüfverfahren als auch für Eich- oder Prüfverfahren Dritter verwendet werden.

Anhang A.4.1 Übergabe an die Eich- oder Prüforganisation und Übergabe von Schlüsselmaterial

Der Zähler und das zugehörige Schlüsselmaterial der Rolle "Eichung und Prüfung" werden der Eich- oder Prüforganisation zur Verfügung gestellt.

Im Key-Management-System ist das Schlüsselmaterial für die Rolle "Eichung und Prüfung" als *aktiv* gekennzeichnet. *Aktiv* bedeutet, dass das Schlüsselmaterial für diese Rolle ausgegeben wurde und dass eine Aktualisierung dieses ausgegebenen Schlüsselmaterials durchgeführt werden muss, sobald dieser Zähler wieder in den Betriebsmodus versetzt wird.

Die Übergabe des Schlüsselmaterials an eine Eich- oder Prüforganisation kann z.B. über eine direkte Anbindung an das Key-Management-System erfolgen. Alternativ kann das bereitgestellte Schlüsselmaterial des Zählers exportiert werden und einen sicheren "Offline-Prozess" durchlaufen. Dies kann z.B. ähnlich dem in "Verfahren zur Bereitstellung von kryptographischem Schlüsselmaterial (beim Hersteller)" beschriebenen Transferprozess sein.

Anhang A.4.2 Bereitstellung eines sicheren Eich- und Prüfmodus

Die Authentifizierung zwischen der Eich- oder Prüforganisation und dem Zähler muss durchgeführt werden. Hierfür wird das mitgelieferte Schlüsselmaterial verwendet. Nach erfolgreicher Authentifizierung kann die Eich- oder Prüforganisation den Zähler mit den entsprechenden Befehlen in einen Eichmodus oder einen Prüfmodus versetzen. Die gesamte Kommunikation zwischen dem Zähler und der Eich- oder Prüforganisation muss authentifiziert werden. Das übergebene Schlüsselmaterial wird verwendet.

In diesem Zustand kann die Eichung oder Prüfung des Messgeräts erfolgen.

Nach einer erfolgreichen Eichung oder Prüfung muss der Zähler mit einem entsprechenden Befehl in den Modus *"Normalbetrieb*" zurückgesetzt werden. Dieser letzte Schritt ist von der Eich- oder Prüforganisation durchzuführen, da der gesicherte Eichmodus außerhalb der Eich- oder Prüforganisation möglicherweise nicht verfügbar ist.

Der Zähler muss die Funktion "Eichung und Prüfung" automatisch deaktivieren, wenn es in den normalen Betriebsmodus wechselt.

Anhang A.4.3 Übertragung in den Betriebsmodus

Der Zähler wird von der Eich- oder Prüforganisation zurückgegeben und kann wieder normal verwendet werden. Bei der Rückgabe wird das Schlüsselmaterial für die Rolle "Eichung und Prüfung" im Key-Management-System als *"Aktualisierung*" gekennzeichnet.

Sobald der Zähler im Feld installiert ist und vom Zentralen System erreicht werden kann, wird das Schlüsselmaterial für "Eichung und Prüfung" durch die Rolle "Zentrales System Read-Write" aktualisiert. Außerdem wird die Funktion "Eichung und Prüfung" vom Zentralen System wieder aktiviert.

Bei Zählern, die bei der Installation keine Online-Verbindung haben, kann die Rolle "Eichung und Prüfung" mit neuem Schlüsselmaterial versehen und mit einem Handbediengerät über die Rolle "Wartung" reaktiviert werden.

Anhang A.5 Entsorgungsprozess

Wenn ein Zähler oder ein (Hybrid-)Gateway entsorgt wird, blockiert das Zentrale System zunächst die Kommunikation mit diesem. Typische Schritte sind:

- Deaktivierung des Geräts im MDMS
- Sperren des Zugangs zu den Kommunikationsnetzen, z.B. durch Sperren der SIM-Karte
- Schlüssel deaktivieren im Key-Management-System
- Entfernen von nicht mehr benötigten Informationen im Zentralen System

Wenn ein Zähler für einen anderen Kunden wiederverwendet werden soll, müssen die personenbezogenen Daten des vorherigen Kunden entfernt werden.

Nach der Entfernung eines (Hybrid-)Gateways sollte dieses auf sichere Weise physisch vernichtet werden, damit die darauf gespeicherten Daten nicht wiederhergestellt werden können.

Bei Zählern sollte der Betreiber auf der Grundlage einer Risikobewertung entscheiden, ob sie auf sichere Weise physisch vernichtet werden müssen. Der Zähler enthält personenbezogene Daten von nur einem Kunden. Die auf dem Zähler gespeicherten Schlüssel sind in der Regel eindeutig und werden im Zentralen System deaktiviert. Daher sind die Risiken geringer als bei einem (Hybrid-)Gateway.

Anhang B Glossar

Das Glossar dient der Erläuterung spezieller Begriffe und Abkürzungen in diesem Dokument. Ausführliche Beschreibungen von Prüfverfahren, Hintergrundinformationen oder Details zu kryptographischen Methoden finden Sie in der empfohlenen Literatur.

Anwendungsschicht	**OSI**-Schicht 5-7.
Ausfallsicher	Konstruktionsprinzip, bei dem eine sicherheitsrelevante Konstruktion die Vertraulichkeit und Integrität des Systems im Falle von Ausfällen garantieren kann.
Authentifizierung	Bei der Authentifizierung wird zwischen der **Authentifizierung von Entitäten** (z.B. einer Person oder eines Geräts) und der **Authentifizierung von Nachrichten** unterschieden. Die Authentifizierung dient der Überprüfung der **Integrität** der Kommunikationspartner oder der **Datenintegrität**.
Authentifizierung von Entitäten	Überprüfung der Identität und **Integrität** der Kommunikationspartner (z.B. der Nutzer am Zähler). Außerdem wird überprüft, ob die Kommunikationspartner während einer Sitzung noch aktiv sind. Siehe auch **Passwort-Authentifizierung** und **starke Authentifizierung**.
Authentizität	Richtigkeit der Herkunft.
Bidirektional	Funktionsweise in zwei Richtungen. Siehe auch **bidirektionale Schnittstelle**.
Bidirektionale Schnittstelle	Die Signale können sich während der Datenübertragung in beide Richtungen bewegen.
Blockchiffre	Eine kryptografische Verschlüsselungsmethode zur Verschlüsselung von Nachrichten mit fester (Block-)Länge.
Broadcast	Datenübertragungstechnik, bei der eine Nachricht gleichzeitig an alle Teilnehmer des Netzes übertragen wird. Mit einem **Multicast** wird die Nachricht an eine Gruppe ausgewählter Teilnehmer im Netz gesendet. Bei einem **Unicast** wird die Nachricht an genau einen Netzwerkteilnehmer gesendet.
BSI	Bundesamt für Sicherheit in der Informationstechnik

DAVID-VO	Österreichische Gesetzgebung: Datenformat- und VerbrauchsinformationsdarstellungsVO 2012. Dieser Katalog bezieht sich auf die Version DAVID-VO 2012 Design.
Digitale Signatur	Um die **Integrität** der Quelle zu gewährleisten. Bei der Erstellung einer digitalen Signatur wird zunächst ein **Hash-Wert** der Datei berechnet. Der Absender erzeugt die digitale Signatur, indem er diesen Hash-Wert mit dem geheimen Schlüssel verschlüsselt. Der Empfänger prüft die digitale Signatur mit dem öffentlichen Schlüssel und vergleicht den **Hashwert** der empfangenen Datei. In der Praxis werden digitale Signaturen mit auf **elliptischen Kurven** (EC) basierenden Algorithmen erzeugt.
Display	Siehe *Kapitel B.*
EC	Elliptische Kurve. Siehe auch ECRYPT [15].
Eindringungserkennungssystem	Ein Eindringungserkennungssystem überwacht das Verhalten von Komponenten entweder auf der Komponente selbst oder durch Überwachung der Kommunikation. Bekannte Angriffsmuster oder Anomalien können erkannt und gemeldet werden.
EPRI	Forschungsinstitut für elektrische Energie (Electric Power Research Institute)
Fuzzing-Test	Zur Qualitätssicherung von Software für sichere Netzkommunikation wird ein Fuzzing-Test durchgeführt. Dies geschieht durch die Erzeugung einer großen, meist zufälligen Datenmenge, die auch fehlerhafte Datenpakete enthalten kann, die strukturiert in den Datenverkehr eingebracht werden. Eine detaillierte Einführung in das Thema Fuzzing findet sich in [15].
Gateway	Siehe Kapitel B.
Gerät	Der Begriff "Gerät" kann sich sowohl auf das Gateway als auch auf den Zähler beziehen. Im Abschnitt Empfehlung und Anleitung zur Umsetzung sind weitere Informationen enthalten.
GPRS	General Packet Radio Service.
HAN	Home Area Network.
Handbediengerät	Ein Werkzeug, das von einem Servicetechniker verwendet wird, um Einstellungen zu ändern und Informationsabfragen über die Wartungsschnittstelle eines Zählers oder Gateways zu senden.

Hash-Funktion	Eine Funktion, die eine Nachricht auf eine Bitfolge (d.h. einen **Hash-Wert**) fester Länge abbildet. Siehe **Kryptographische Hash-Funktion**.
Hash-Wert	Ausgabe einer **(kryptographischen) Hash-Funktion**.
Hybride Verschlüsselung	Da die **Public-Key-Kryptographie** in Bezug auf Schlüssellänge, Rechenleistung usw. ressourcenintensiv ist, werden Algorithmen wie RSA nur in so genannten Hybridverfahren verwendet. Zunächst wird ein zufälliger symmetrischer Sitzungsschlüssel erzeugt (z.B. ein 128-Bit-AES-Schlüssel). Dann wird der Sitzungsschlüssel verschlüsselt mit dem öffentlichen Schlüssel des Empfängers gesendet. Die eigentlichen Nachrichten werden dann unter Verwendung des Sitzungsschlüssels mit der entsprechenden symmetrischen Chiffre (z.B. AES) ver- und entschlüsselt.
IETF	Internet Engineering Task Force.
IKT-Sicherheit	Sicherheit in der Informations- und Kommunikationstechnologie.
IMA-VO	Österreichische Gesetzgebung: Intelligente Messgeräte-AnforderungsVO. Dieser Katalog bezieht sich auf die Fassung "339. Verordnung ausgegeben am 25. Oktober 2011 Teil II".
Integrität	Die Integrität einer Nachricht bedeutet Schutz vor Manipulationen. Siehe auch **Authentifizierung**.
Integrität der Daten	Siehe **Integrität** und **Nachrichtenauthentifizierung**.
ISO 27001	ISO-Norm für IKT-Sicherheit.
Konfigurationsmanagementsystem	Das Konfigurationsmanagementsystem ist das System beim Hersteller, das den Lebenszyklus des Geräts von der Entwicklung über die Fertigung bis zur Beschaffung verwaltet. Das System umfasst insbesondere die Verwaltung von Software und Quellen für (kundenspezifische) Konfigurationen eines Geräts.
Kryptographie	Der Bericht der ECRYPT über Algorithmen, Schlüsselgrößen und Parameter [16] enthält Informationen über den Stand der Technik in der Kryptographie.
Kryptographische Hash-Funktion	Kryptografische Hash-Funktionen müssen sich wie Einwegfunktionen verhalten und kollisionssicher und stark kollisionssicher sein. Änderungen in der Eingabenachricht

	müssen zu einer signifikanten Änderung des Hashwerts führen. Beispiel: SHA-256. Siehe auch ECRYPT [16].
LAN	Local Area Network.
Lesen-Schreiben	Der Benutzer hat Lese- und Schreibrechte.
MAC	Message Authentication Code. Zur Überprüfung der Datenintegrität. Beispiele: CMAC, GMAC. Siehe auch ECRYPT [16].
Multicast	Mit einem **Multicast** wird die Nachricht an eine Gruppe ausgewählter Teilnehmer im Netz gesendet. Ein **Multicast** ist ein Spezialfall eines **Broadcasts**.
Nachrichtenauthentifizierung	Die **Authentizität** der Nachricht, d.h. die Echtheit der Nachricht, muss gewährleistet sein. Dies geschieht entweder durch Anhängen eines Nachrichtenauthentifizierungscodes (z.B. AES-CBC-CMAC) oder durch Verwendung einer Blockchiffre in einem authentifizierenden Betriebsmodus (z.B. AES-CCM, AES-GCM).
NESCOR	National Electric Sector Cybersecurity Organization Resource. Programm der US-Organisation **EPRI**. Siehe auch [17].
NIST	National Institute of Standards and Technology.
Nonce	Ein Nonce ist eine eindeutige, zufällig generierte Zeichenfolge, die genau einmal verwendet werden muss (im mittelalterlichen Englisch bedeutet der gebräuchliche Ausdruck "for the nonce" "für dieses eine Mal"). Wird an die Nachricht angehängt, um **Wiedereinspielangriffe** zu erkennen oder zu verhindern.
Nur Lesen	Der Benutzer kann Daten lesen. Es ist nicht erlaubt, neue Informationen zu schreiben oder bestehende Informationen zu ändern.
OSI	Open Systems Interconnection. Referenzmodell für die Netzkommunikation.
Passwort-Authentifizierung	Der Benutzer meldet sich mit dem Benutzernamen und dem Passwort oder der PIN am Gerät an. Das Gerät selbst braucht sich nicht zu authentifizieren. Diese Methode ist besonders anfällig für den Diebstahl von Kennwörtern durch Social Engineering-Angriffe. Für kritische Bereiche wird eine gegenseitige/starke Authentifizierung empfohlen.

Penetrationstest	Das **EPRI**-Programm **NESCOR** ist eine der Organisationen, die mit ihrem "AMI Penetration Test Plan" Richtlinien für Penetrationstests bereitstellt.
Persönliche Daten	Siehe Datenschutzverordnung. Beispiel: Lastprofilwerte.
PLC	Power Line Communication.
Produktlebenszyklus	Der Produktlebenszyklus umfasst die Phasen Entwurf, Entwicklung, Produktion und Beschaffung, Betrieb und Außerbetriebnahme eines Geräts.
Protokolldatei	Ereignisse beim Betrieb von Zählern werden in einer oder mehreren Protokolldateien aufgezeichnet. Ein anderer Begriff ist Protokoll. In einer fortlaufenden Protokolldatei können Einträge (mit entsprechenden Berechtigungen) überschrieben werden, nachdem der reservierte Speicherplatz für Protokolle erschöpft ist.
Public-Key-Infrastruktur	System zum Ausstellen, Verteilen und Überprüfen von Zertifikaten.
Public-Key-Kryptographie	Eine kryptografische Methode, bei der ein öffentlicher Schlüssel für die **Verschlüsselung** und die Überprüfung **digitaler Signaturen** bereitgestellt wird. Zu jedem öffentlichen Schlüssel gibt es einen entsprechenden privaten Schlüssel, der unter keinen Umständen veröffentlicht werden darf (d.h. der private Schlüssel muss geheim gehalten werden). Der private Schlüssel wird zum Entschlüsseln und **digitalen Signieren** von Nachrichten verwendet. Die Kryptographie mit öffentlichen Schlüsseln wird nicht zur direkten Verschlüsselung von Nachrichten verwendet. Vielmehr wird bei der so genannten hybriden Verschlüsselung ein symmetrischer Sitzungsschlüssel verschlüsselt unter dem öffentlichen Schlüssel gesendet. Die Authentizität eines öffentlichen Schlüssels soll mit Zertifikaten in einer **Public Key Infrastructure** (PKI) sichergestellt werden. Siehe auch ECRYPT [16]. Die bekannteste Methode der Verschlüsselung mit öffentlichen Schlüsseln ist RSA.

	Im Prinzip ist es möglich, mit RSA digital zu signieren; in der Praxis werden digitale Signaturen jedoch mit auf elliptischen Kurven (**EC**) basierenden Algorithmen erstellt.
RFC	Requests for Comments (Bitte um Kommentare). Veröffentlicht von der **IETF**.
Robustheitstest	Zur Qualitätssicherung der Stabilität des Systemaufbaus wird ein Robustheitstest durchgeführt. Dabei wird insbesondere die Fehlertoleranz getestet.
Rolle	Siehe Abschnitt B.3.
Schlüsselmaterial	Zum **Schlüsselmaterial** gehören alle kryptografischen Schlüssel. Beispiele sind Hauptschlüssel, symmetrische Schlüssel, **Sitzungsschlüssel**, private Schlüssel und öffentliche Schlüssel (in der **Public-Key-Kryptographie**).
Sitzungsschlüssel	Symmetrischer Schlüssel, der für die Verschlüsselung aller Nachrichten innerhalb eines begrenzten Zeitrahmens (Sitzung) verwendet wird.
Starke Authentifizierung	Bei der starken Authentifizierung müssen sich beide Seiten authentifizieren und damit ihre Identität nachweisen. Häufig werden Challenge-Response-Protokolle verwendet. Andere gängige Methoden verwenden Zertifikate.
Techniker-Menü	Eine Funktion des Geräts, die es einem Servicetechniker ermöglicht, Einstellungen zu ändern und Informationen auf dem lokalen Display über Tastatureingaben abzurufen.
Überwachungs-system	Siehe **Eindringungserkennungssystem**.
Unicast	Bei einem **Unicast** wird die Nachricht an genau einen Netzwerkteilnehmer gesendet. Siehe auch **Broadcast**.
Unidirektional	Funktioniert nur in eine Richtung. Siehe auch **unidirektionale Schnittstelle**.
Unidirektionale Schnittstelle	Die Signale können sich während der Datenübertragung nur in eine Richtung bewegen, z.B. vom Zähler zum Kunden an der Kundenschnittstelle.
Verschlüsselung	Die Nachricht wird mithilfe eines kryptografischen Verfahrens in eine Zeichenkette umgewandelt, die als Chiffretext bezeichnet wird und für einen Angreifer unlesbar ist. Die Entschlüsselung ist

	die Rückverwandlung des verschlüsselten Textes in den ursprünglichen Nachrichtentext; sie erfolgt mit demselben Schlüssel (symmetrische Kryptographie) oder mit dem privaten Schlüssel (**Public-Key-Kryptographie**).
Versionierungs-prozess	Ein Versionierungsprozess ist Teil des **Konfigurationsmanagements**.
Versorgungszähler	Zum Beispiel Zähler für Gas-, Wasser- und Wärmeverbrauch.
Vertraulichkeit	Nur ausgewählte Benutzer können auf vertrauliche Nachrichten zugreifen. Dies geschieht häufig durch **Verschlüsselung** von Nachrichten, wobei nur autorisierte Personen Zugang zum geheimen **Schlüsselmaterial** erhalten.
Vier-Augen-Prinzip	Doppelte Kontrolle. Entscheidungen müssen von mehr als einer Person getroffen werden.
WAN	Wide Area Network.
Wartungs-schnittstelle	Siehe Kapitel B.
Wiedereinspiel-angriff	Der Angreifer zeichnet die Daten einer Sitzung auf und verwendet sie später, um sich als eine andere Identität auszugeben.
Zähler	**Zähler** bezieht sich in erster Linie auf den Stromzähler. Falls erforderlich, werden Stromzähler und **Versorgungszähler** ausdrücklich unterschieden.
Zertifikat	Ein digitales Zertifikat ist eine Datei, die die Überprüfung der Authentizität eines Kommunikationsteilnehmers oder einer Nachricht ermöglicht. Siehe **Public-Key-Infrastruktur**.

Anhang C Literatur

[1] E-Control Austria, „Risikoanalyse für die Informationssysteme der Elektrizitätswirtschaft,“ 2014 February 27. [Online]. Available: https://www.e-control.at/publikationen/publikationen-strom/studien/ikt-risikoanalyse.

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI), „BSI TR-03109-1. Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems. Version 1.1,“ Bonn, Germany, September 2021.

[3] Internet Engineering Task Force, „RFC 2119: Key words for use in RFCs to Indicate Requirement Levels," 1997. [Online]. Available: http://www.ietf.org/rfc/rfc2119.txt.

[4] National Institute for Sandards and Technology (NIST), „Special Publication 800-57 Part 1 Rev. 5: Recommendation for Key Management," 2020.

[5] Bundesamt für Sicherheit in der Informationstechnik (BSI), „BSI TR-03116, Part 3, Kryptographische Vorgaben für Projekte der Bundesregierung – Intelligente Messsysteme," 2023.

[6] Bundesamt für Sicherheit in der Informationstechnik (BSI), „BSI TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen," 2022.

[7] Bundesamt für Sicherheit in der Informationstechnik, „Anwendungshinweise und Interpretationen zum Schema, AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3.0," Bonn, Germany, 2013.

[8] Bundesamt für Sicherheit in der Informationstechnik, „Anwendungshinweise und Interpretationen zum Schema, AIS 31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3.0, Bonn, Germany, May 2013.," Bonn, Germany, 2013.

[9] National Institute of Standards and Technology (NIST), „FIPS PUB 186-4, Digital Signature Standard (DSS)," 2013.

[10] National Institute of Standards and Technology (NIST), „Annex C: Approved Random Number Generators for FIPS PUB 140-2," 2021.

[11] Österreichischen Normungsinstitut, „ÖNORM A-7700 Sicherheitstechnische Anforderungen an Webapplikationen," 2019. [Online].

[12] Open Web Application Security Project (OWASP), „Input Validation Cheat Sheet," [Online]. Available: https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html.

[13] National Institute of Standards and Technology (NIST), „FIPS PUB 140-3, Security Requirements for Cryptographic Modules," 2019.

[14] OASIS, „PKCS #11: Cryptographic Token Interface Standard.," 2015. [Online]. Available: https://www.oasis-open.org/standards.

[15] J. D. C. M. Ari Takanen, „Fuzzing for Software Security Testing and Quality Assurance (1 ed.)," Artech House, Inc, Norwood, MA, USA, 2008.

[16] ECRYPT - CSA, „D5.4 Algorithms, Key Size and Protocols Report," 2018.

[17] Electric Power Research Institute, „National Electric Sector Cybersecurity Organization Resource," [Online]. Available: http://smartgrid.epri.com/NESCOR.aspx.