Anforderungskatalog

Ende-zu-Ende Sicherheit Smart Metering

In Auftrag gegeben durch Oesterreichs Energie, Brahmsplatz 3, 1041 Wien

Ausgeführt durch das European Network for Cyber Security, P.O. Box 16068, 2500 BB Den Haag, Niederlande

Versionsnummer:	2018-1.1
Ersteller:	Projektgruppe End2End Security Smart Metering
Ausstellungsdatum:	31.Jänner 2018
Anzahl der Seiten:	86

Medieninhaber:

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

AUTOREN: PG END2END SECURITY SMART METERING, Oesterreichs Energie

MICHAEL JOHN, European Network for Cyber Security (Projektleitung ENCS)

WOLFGANG LÖW, EVN (Vorsitzender PG)

JOHANN BERNHARDT, Energie Burgendland AG

CHRISTOPH EBERL, Wiener Netze GmbH

PETER EDER-NEUHAUSER, Wiener Netze GmbH

BERNHARD EGGER, Energie AG OÖ Data GmbH

MANFRED FARTHOFER, Salzburg AG

FRÉDÉRIC GIERLINGER, KELAG

BERNHARD LEITNER, TINETZ-Tiroler Netze GmbH

PHILIPP MEYER, IKB AG

BERNHARD MORSCHER, VKW

FRIEDRICH NEURAUTER, TINETZ AG

ANDREAS ORLITSCH, E-Steiermark Technik GmbH

THOMAS PFEIFFER, Linz Strom Netz GmbH

RENE SCHMID, STW Klagenfurt

ANDREA STEINBAUER, E-Steiermark Technik GmbH

Inhaltsverzeichnis

A. Aufbau des Anforderungskataloges

A.1 Geltungsbereich

Dieser Katalog beschreibt die Mindest-Anforderungen an die Hersteller bei der Ausschreibung von Stromzähler, Gateway und Zentralem System, sowie deren Kommunikationsverbindungen, die im Smart Metering Bereich mit Ende-zu-Ende Sicherheit in Österreich eingesetzt werden sollen. Die Verwendung von Ende-zu-Ende Sicherheit entspricht den empfohlenen Maßnahmen der Risikoanalyse für die Informationssysteme der Elektrizitätswirtschaft vorgestellt von der E-Control Austria (ECA) am 27.Februar 2014 [1].

Der Begriff Smart Metering ist nicht zu verwechseln mit dem „Smart Grid“ Begriff; die Sicherheit von beispielsweise Steuerungs- und Telekommunikationssystemen für elektrische Übertragungs- und Verteilnetze ist nicht Teil dieses Anforderungskataloges. Die zugrundeliegende Ende-zu-Ende Sicherheitsarchitektur für Smart Metering wird in Kapitel B beschrieben.

Die in diesem Katalog vorgesehenen Maßnahmen beruhen auf dem heutigen Stand der Technik im Bereich IKT Sicherheit, das heißt der Sicherheit in der Informations- und Kommunikationstechnik. Die Ziele der IKT Sicherheit sind die Gewährleistung der Authentizität und damit Integrität von Informationen im digitalen Datenverkehr[1] sowie die Geheimhaltung vertraulicher Daten. Die Formulierungen sicher/gesichert/Sicherheit sind in diesem Katalog im Sinne der IKT Sicherheit zu verstehen. Andere Interpretationen, beispielsweise Sicherheit im Sinne der Betriebssicherheit oder Arbeitssicherheit, werden explizit gekennzeichnet.

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

A.2 Wortlaut

Dieser Anforderungskatalog folgt bei der Unterscheidung zwischen normativen und informativen Inhalten der Terminologie der Technischen Richtlinie TR-03109 (beispielweise [2, Abschnitt 1.5]) des deutschen Bundesamts für Sicherheit in der Informationstechnik. Schlüsselwörter werden gemäß RFC2119 [3] in Großbuchstaben gedruckt:

- MUSS bedeutet, dass es sich um eine normative Anforderung handelt.
- DARF NICHT / DARF KEIN / DARF NUR / DARF WEDER … NOCH bezeichnen den normativen Ausschluss einer Eigenschaft/von Eigenschaften.

[1] Hier ist Datenverkehr im Sinne der Ende-zu-Ende Smart Meter Architektur (siehe Kapitel B) zu verstehen.

- SOLL beschreibt eine dringende Empfehlung. Abweichungen zu diesen Festlegungen müssen begründet werden.
- SOLL NICHT / SOLL KEIN kennzeichnet die dringende Empfehlung, eine Eigenschaft auszuschließen. Abweichungen zu diesen Festlegungen müssen begründet werden.
- KANN / DARF bedeutet, dass die Eigenschaften fakultativ oder optional sind.

Sämtliche Bezeichnungen sollen geschlechtsneutral verstanden werden. Wurde nur auf ein Geschlecht verwiesen, so gilt die Formulierung auch für das andere Geschlecht.

A.3 Aufbau der Anforderungen

Jede Anforderung ist mit einem Anforderungskennzeichen (Anf._ID) gekennzeichnet und enthält die drei Punkte

1. Anforderung
2. Empfehlung und Umsetzungserläuterungen
3. Empfohlene Qualitätssicherungsmaßnahme

welche wie folgt definiert sind:

1. Anforderung: Eine *Anforderung* bezeichnet ein Erfordernis oder eine Erwartung, das oder die festgelegt, üblicherweise vorausgesetzt oder verpflichtend ist. Diese Ausschreibungsunterlage verwendet den Begriff *Anforderung* im Sinne einer normativen, also verpflichtenden, Anforderung.
2. Empfehlung und Umsetzungserläuterungen: *Empfehlungen* stellen Möglichkeiten dar, wie die Anforderung umgesetzt werden kann. Die Anforderung darf auch gleichwertig gelöst werden, vorausgesetzt, dass die Gleichwertigkeit der Lösung schriftlich und ausführlich begründet wird. Die *Umsetzungserläuterungen* stellen Beispiele und Erklärungen dar, wie die Anforderung zu interpretieren ist.
3. Empfohlene Qualitätssicherungsmaßnahme: *Empfohlene Qualitätssicherungsmaßnahmen* enthalten Vorschläge, wie die Anforderung zu überprüfen ist. Die Zielsetzung hierbei ist, Empfehlungen für sowohl die Prüfstelle als auch den Hersteller auszusprechen, um den Hersteller auf zu erwartende Prüfprozesse hinzuweisen. Die hier empfohlenen Testprozeduren werden in Anhang B näher erläutert.

A.4 Gültigkeit

Die Anforderungen gelten, wenn nicht anders angegeben, für den Zähler, das Gateway und das Zentrale System.
Die Anforderungen für Sicherheit der Software im Zentralen System sind als Basis zu verstehen und sind durch die IKT Sicherheitsrichtlinien des Systembetreibers zu ergänzen.

Anforderungen mit einer Endung des Anforderungskennzeichens auf „.ZL“ gelten speziell für den Zähler.
Anforderungen mit einer Endung des Anforderungskennzeichens auf „.GW“ gelten speziell für das Gateway.
Anforderungen mit einer Endung des Anforderungskennzeichens auf „.ZS“ gelten speziell für das Zentrale System.
Referenzen auf eine Gruppe werden beispielsweise mit SXR_01.* gekennzeichnet.

A.5 Gliederung

Die Anforderungen in diesem Dokument sind wie folgt kategorisiert:

- Kapitel 0~~C~~ enthält Anforderungen für das Smart Metering System. Insbesondere werden die folgenden Bereiche abgedeckt.
    - Allgemeine Sicherheitsanforderungen
        - Zukunftssicherheit
        - Schnittstellen-Reduzierung
        - Kryptografische Algorithmen
    - Datenintegrität
    - Lokale Sicherung
    - Zugangskontrolle
    - Vertraulichkeit
    - Auditierung und Protokolle
    - Produktlebenszyklus-Management
- Anhang A enthält Beschreibungen von ausgewählten Prozessen. Diese dienen als Beispiele, wie ausgewählte Anforderungen im Sinne der Ende-zu-Ende Sicherheit umgesetzt werden können, und sind nicht im normativen Sinne sondern als Verständnishilfe zu interpretieren.
- Anhang B enthält ein Verzeichnis mit Erläuterungen der im Katalog verwendeten Fachbegriffe und Abkürzungen.
- Anhang C enthält die verwendeten Referenzen und Richtlinien.

B. Ende-zu-Ende Sicherheitsarchitektur

B.1 Smart Metering Architektur

Die generische Architektur des Smart Metering Systems ist in Abbildung 1 dargestellt. Hierbei sind lediglich die minimalen Schnittstellen des Systems beschrieben. Die Beschreibungen orientieren sich an den Vorgaben der IMA-VO.

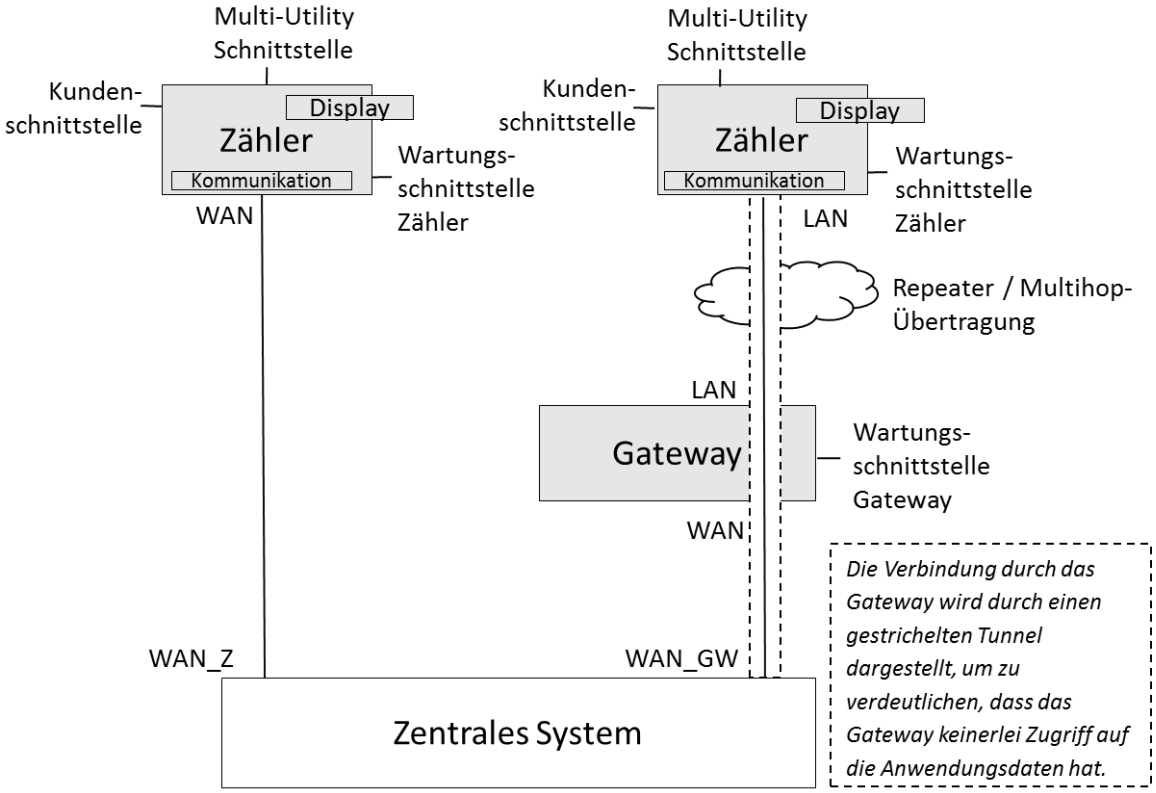

Abbildung 1: Ende-zu-Ende gesicherte Smart Meter Architektur

Die Ende-zu-Ende gesicherte Smart Meter Architektur erlaubt zwei Zählertypen: zum einen Stromzähler, die über eine WAN-Schnittstelle an das Zentrale System angeschlossen sind, und zum anderen Stromzähler, die über ein lokales Netzwerk (LAN) an einen Datenkonzentrator/Datensammler angeschlossen werden, der als *Gateway* zum Zentralen System fungiert. Unabhängig von der gewählten Lösung muss jegliche Kommunikation vom Zentralen System zu individuellen Zählern Ende-zu-Ende gesichert durchgeführt werden. Dies bedeutet insbesondere, dass ein Datenkonzentrator/Datensammler keine eigenen Berechtigungen besitzt, um Informationen vom Zähler auszulesen, Funktionen aufzurufen oder Einstellungen am Zähler zu ändern. Kommunikation vom Zähler wird transparent durch das Gateway zum Zentralen System geleitet.

Aus diesem Grund wurde anstelle des Begriffs „Datenkonzentrator/Datensammler“ die Bezeichnung „Gateway“ gewählt.

Hervorzuheben ist auch die Eigenschaft, dass das Gateway keinerlei kryptografisches Schlüsselmaterial besitzt, um Daten, welche zwischen den Zählern und dem Zentralen System ausgetauscht werden, zu entschlüsseln, zu verändern oder zu analysieren.

Sollten Zähler und WAN- oder LAN-Kommunikationsmodul durch physikalisch separierte Komponenten realisiert sein, so sind die Schnittstellen zwischen diesen Komponenten allein mit den in diesem Dokument zugelassenen kryptografischen Verfahren zu sichern.

Für eine Implementierung der Zählerinfrastruktur ist auch die Umsetzung eines Multilayer-Security Konzeptes empfohlen. Zusätzlich zu der Ende-zu-Ende gesicherten Anwendungsschicht zwischen Zähler und Zentralen Systemen, können auch kryptographische Verfahren zur Sicherung von unteren Schichten eingesetzt werden. Sicherheitsvorgaben für ein solches Konzept sind jedoch nicht Teil dieses Dokumentes.

Zähler:

Der Begriff *Zähler* bezieht sich in erster Linie auf den Stromzähler. Dieser ist entweder mit einer WAN- oder LAN-Schnittstelle ausgestattet. Spartenzähler beispielsweise für die Bereiche Gas, Wasser, Wärme, können über die Multi-Utility-Schnittstelle an den Stromzähler angebunden werden.

Kommunikation: Der Zähler besitzt entweder eine LAN- oder eine WAN-Schnittstelle.

Display: Die Anzeigen auf dem integrierten Verbrauchsdisplay des Zählers. Es finden die Anforderungen der IMA-VO Anwendung.

Kundenschnittstelle: Die Kundenschnittstelle stellt dem Verbraucher nach IMA-VO aktuelle Verbrauchsinformationen zur Verfügung. Diese Schnittstelle darf ausschließlich mit unidirektionaler Kommunikation realisiert werden.

Multi-Utility-Schnittstelle: Über die Multi-Utility-Schnittstelle am Stromzähler können andere Zähler (z.B. Gas, Wasser, Wärme) angebunden werden. Die Schnittstelle muss mit bidirektionaler Kommunikation realisiert werden.

Wartungsschnittstelle: Der Zugriff auf den Stromzähler innerhalb der Eichstelle, in einem Testlabor, oder vor Ort von einem Techniker erfolgt über die Wartungsschnittstelle am Stromzähler. Die Schnittstelle muss mit bidirektionaler Kommunikation realisiert werden.

LAN-Schnittstelle: Die LAN-Schnittstelle am Zähler stellt die Verbindung zu einem Gateway dar, welches wiederum die Verbindung zum Zentralen System realisiert. Die Schnittstelle muss mit bidirektionaler Kommunikation realisiert werden.

WAN-Schnittstelle: Die WAN-Schnittstelle am Zähler stellt eine direkte Verbindung zum Zentralen System dar. Die Schnittstelle muss mit bidirektionaler Kommunikation realisiert werden.

Gateway:

Das Gateway ist die Komponente innerhalb der Smart Metering Architektur, welche eine transparente Kommunikationsverbindung zwischen dem Zentralen System und Zähler realisiert. Hierbei ist „transparent“ im Sinne der Ende-zu-Ende Sicherheit zu verstehen.

Der aktuelle Begriff *Gateway* kann auch als Teilfunktionalität auf einem Datenkonzentrator bzw. Datensammler verstanden werden, welche die Erfordernisse hinsichtlich Sicherheit in Bezug auf Smart Metering abbildet.

Wartungsschnittstelle: Über die Wartungsschnittstelle am Gateway erfolgt der Zugriff auf das Gateway innerhalb eines Testlabors oder vor Ort von einem Techniker. Die Schnittstelle muss mit bidirektionaler Kommunikation realisiert werden.

LAN-Schnittstelle: Die LAN-Schnittstelle am Gateway stellt Verbindungen zu Zählern her. Die Schnittstelle muss mit bidirektionaler Kommunikation realisiert werden.

WAN-Schnittstelle: Die WAN-Schnittstelle am Gateway stellt die Verbindung zum Zentralen System her. Die Schnittstelle muss mit bidirektionaler Kommunikation realisiert werden.

Zentrales System:

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

WAN_GW-Schnittstelle: Die WAN_GW-Schnittstelle am Zentralen System stellt die Verbindungen zu den Gateways her. Die Schnittstelle muss mit bidirektionaler Kommunikation realisiert werden.

WAN_Z-Schnittstelle: Die WAN_Z-Schnittstelle am Zentralen System stellt direkte Verbindungen zu den Zählern her. Die Schnittstelle muss mit bidirektionaler Kommunikation realisiert werden.

B.2 Architektur des Zentralen Systems

Die Architektur des Zentralen Systems in Abbildung 2 beschrieben. Hierbei sind lediglich die minimalen Schnittstellen des Systems beschrieben. Die Pfeile der Verbindungen geben an, ob eine Schnittstelle unidirektional oder bidirektional umgesetzt wird.

Zum Zentralen System gehören Head-End, MDMS und ein Key Management System für die Zählerinfrastruktur. Das Kundenportal ist nicht Teil des Zentralen Systems.

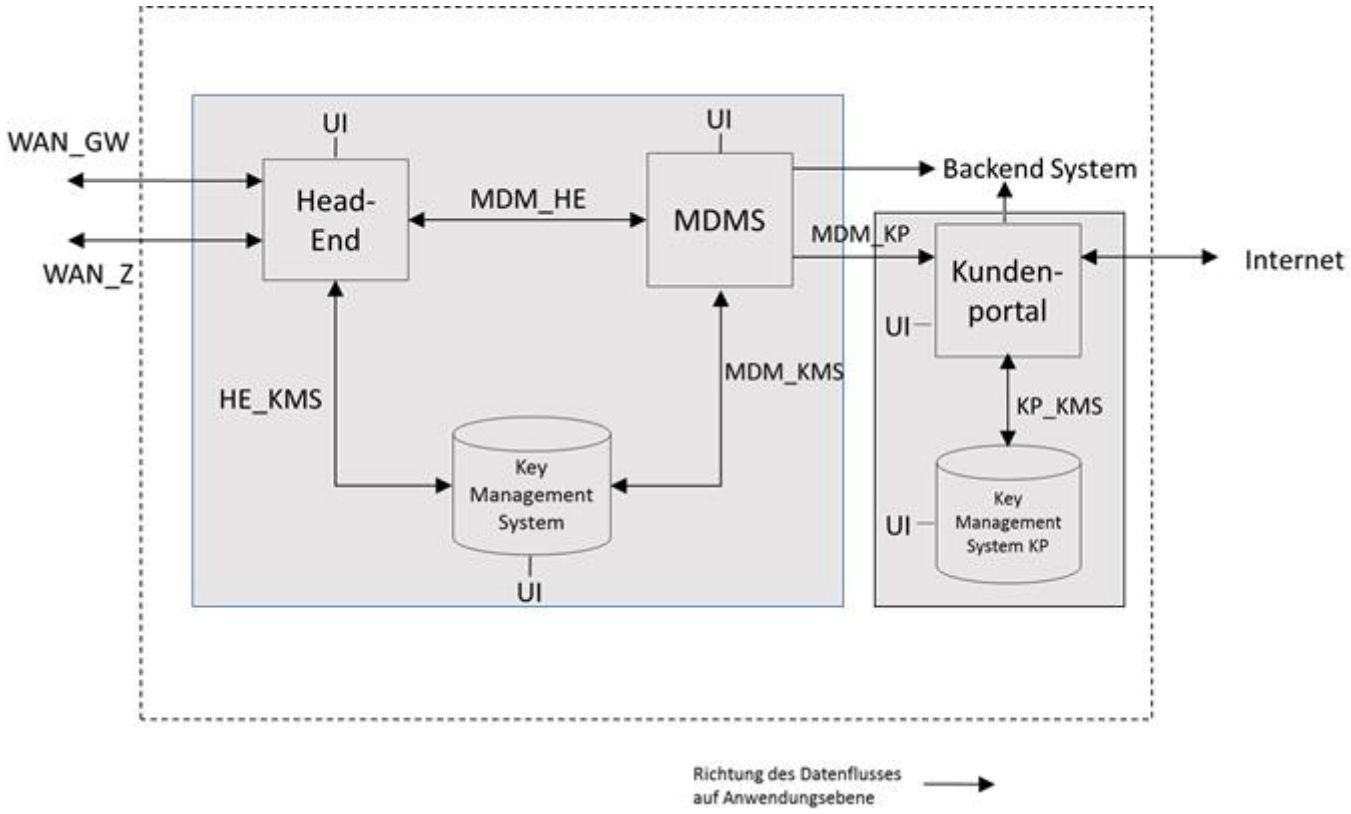

Abbildung 2: Architektur des Zentralen Systems

Head-End System:

Das Head-End kommuniziert mit den Stromzählern bzw. den Gateways, und stellt die Daten dem Meter Data Management System (MDMS) zur Verfügung, bzw. leitet Nachrichten vom MDMS an die Zähler weiter.

Benutzerschnittstelle (UI): Über diese Schnittstelle werden operative Arbeiten und Wartungsarbeiten am Head-End System ausgeführt. Die Benutzerschnittstelle kann auch die Fernwartungsschnittstelle beinhalten.

HE_KMS-Schnittstelle: Diese Schnittstelle erlaubt dem Head-End System, mit dem Key Management System zu kommunizieren.

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

Meter Data Management System:

Das Meter Data Management System (MDMS) speichert, bearbeitet und verwaltet die Zählerdaten, und stellt diese dem Kundenportal sowie internen Betriebsprozessen zur Verfügung. Das MDMS kann weiterhin Funktionen wie Ersatzwertbildung oder Firmwaredateiverwaltung erfüllen.

Benutzerschnittstelle (UI): Über diese Schnittstelle werden operative Arbeiten und Wartungsarbeiten am MDMS ausgeführt. Die Benutzerschnittstelle kann auch die Fernwartungsschnittstelle beinhalten.

Back-End System-Schnittstelle: Diese Schnittstelle bindet das Meter Data Management System an das interne Unternehmensnetzwerk an. Abhängig von den konkreten Anwendungsfällen kann diese Schnittstelle unidirektional sein, also nur Daten vom MDMS an die Unternehmensanwendungen übermitteln, nicht aber umgekehrt.

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

MDM_KMS-Schnittstelle: Diese Schnittstelle erlaubt dem MDMS, mit dem Key Management System zu kommunizieren.

Key Management System:

Das Key Management System verwaltet und schützt kryptografische Schlüssel. Es stellt einen sicheren Speicher für Schlüsselmaterial zur Verfügung und kontrolliert die Autorisierung zur Benutzung des Schlüsselmaterials. Das Key Management System sollte aus unabhängigen Komponenten bestehen, beispielsweise eine Komponente für das Head-End und eine für das Kundenportal.

Benutzerschnittstelle (UI): Über diese Schnittstelle werden Wartungsarbeiten am Key Management System ausgeführt. Es ist nicht empfohlen diese Schnittstelle mit Fernwartungsfunktionalitäten zu versehen.

HE_KMS-Schnittstelle: Diese Schnittstell erlaubt dem Head-End System, mit dem Key Management System zu kommunizieren.

MDM_KMS-Schnittstelle: Diese Schnittstell erlaubt dem MDMS, mit dem Key Management System zu kommunizieren.

KP_KMS-Schnittstelle: Diese Schnittstell erlaubt dem Kundenportal, mit dem Key Management System zu kommunizieren.

Kundenportal:

Das Kundenportal in dieser Architektur ist als Kundenportal des Netzbetreibers (nicht einer Drittpartei) zu verstehen. Das Kundenportal stellt die Zugangsplattform für Kunden und Drittanbieter dar. Das Kundenportal ist die einzige Zone mit direkter Anbindung ans öffentliche Internet. Das Kundenportal zählt nicht zu den Zentralen Systemen, dieses Dokument stellt keine detaillierten Sicherheitsvorgaben für das Kundenportal auf.

Benutzerschnittstelle (UI): Über diese Schnittstelle Wartungsarbeiten am Kundenportal des Netzbetreibers ausgeführt. Die Benutzerschnittstelle kann auch die Fernwartungsschnittstelle beinhalten.

Internet-Schnittstelle: Die Internetschnittstelle ist die Verbindung zum öffentlichen Internet. Kunden und Drittanbieter können über diese Schnittstelle mit dem Kundenportal kommunizieren.

KP_KMS-Schnittstelle: Diese Schnittstell erlaubt dem Kundenportal, mit dem Key Management System zu kommunizieren.

MDM_KP-Schnittstelle: Die MDM_KP Schnittstelle regelt die Kommunikation zwischen MDMS und dem Kundenportal. Diese Schnittstelle kann unidirektional sein um das MDMS vor einem korrumpierten Kundenportal zu schützen.

Back-End System-Schnittstelle: Diese Schnittstelle bindet das Kundenportal an das interne Unternehmensnetzwerk an.

B.3 Rollen

Für eine rollen-basierte Zugangskontrolle werden Rollen und dazugehörige Privilegien sowie deren Anwendungsbereiche in der Architektur definiert. Hierbei sind lediglich die minimal zu unterstützenden Rollen der in der Architektur definierten Komponenten beschrieben. Bei den dargestellten Privilegien handelt es sich um Vorschläge. Die konkrete Ausprägung ist vom Netzbetreiber festzulegen.

B.3.1 Rollen am Zähler

Rollen-bezeichnung	Privilegien	Anwendungs-bereich	Schnittstellen am Zähler
Eich- und Prüfstelle	Die Rolle *Eich- und Prüfstelle* hat folgende Funktionen: Zugriff für Eichstelle, externe Prüfstelle, Marktüberwachung, Sachverständige oder Zertifizierungsstelle. Die Rolle *Eich- und Prüfstelle* hat folgende Berechtigungen: Breaker schalten, Messregister auslesen, Tarifregister schalten, Firmware Update durchführen, Zugriff auf Protokolle, Parametrierung/Konfiguration.	Interne Eichstelle des Netzbetreibers, Externe Prüfstelle, Marktüberwachung, Sachverständige, Zertifizierungsstelle.	Wartungs-schnittstelle
Maintenance	Die Rolle *Maintenance* hat folgende Funktionen: Durchführen von vor-Ort Konfigurationen des Gerätes. Die Rolle *Maintenance* hat folgende Berechtigungen: Firmware Update, Registerauslesen, Konfigurationen des Gerätes (z.B. Setzen der Uhrzeit, Pairing Spartenzähler), Breaker schalten	Handheld Terminal / Techniker Gerät	Wartungs-schnittstelle
Installation	Die Rolle Installation hat folgende Funktionen: Inbetriebnahme bzw. Installation des	Handheld Terminal / Techniker Gerät	Wartungs-schnittstelle

	Zählers durch einen Techniker vor Ort. Die Rolle Installation hat folgende Berechtigungen: Firmware Update, Registerauslesen, Konfigurationen des Gerätes (z.B. Setzen der Uhrzeit, Pairing Spartenzähler). Diese Rolle soll nach erfolgreicher kommunikativer Anbindung deaktiviert werden. Nach erfolgreicher kommunikativer Anbindung des Zählers soll diese Rolle deaktiviert werden. Eine Reaktivierung der Rolle darf ausschließlich über ein gesichertes Kommando stattfinden.		
Kunde	Die Rolle *Kunde* hat folgende Funktionen: Unidirektionale Kundenschnittstelle für die Ausgabe der Verbrauchswerte. Die Rolle *Endverbraucher* hat folgende Berechtigungen: Register mit aktuellen Verbrauchswerten. Hinweis: Der Zugriff auf die Registerwerte KANN hierbei ohne Interaktion des Kunden erfolgen, z.B. permanente Ausgabe der aktuellen Verbrauchswerte auf der Kundenschnittstelle.	Kundenschnittstelle	Kunden-schnittstelle
Anzeige	Die Rolle *Anzeige* hat folgende Funktionen: Erlaubt Auslesen von Informationen,	Handheld Terminal, Externe Prüfstelle, Marktüberwachung	Wartungs-schnittstelle

	welche über das Display angezeigt werden. Die Berechtigung der Rolle *Anzeige* beschränkt sich ausschließlich auf die aktuell am Zählerdisplay abzurufenden Informationen. Beispiele sind aktuelle Verbrauchswerte, Firmwareversion oder Seriennummer. Die Rolle *Anzeige* darf ohne Authentifizierung implementiert werden.		
Zentrales System Read-Only	Die Rolle *Read-Only* hat Lesezugriff auf definierte Speicherbereiche (Register/Lastprofile/etc…).	Zentrales System	WAN oder LAN
Zentrales System Read-Write	Die Rolle *Read-Write* hat Zugriff auf alle Speicherbereiche und Funktionen. Die Rolle kann Privilegien aller Rollen ändern.	Zentrales System	WAN oder LAN

B.3.2 Rollen am Gateway

Rollen-bezeichnung	**Privilegien**	**Anwendungs-bereich**	**Schnittstellen am Gateway**
Maintenance	Die Rolle *Maintenance* hat folgende Funktionen: Durchführen von vor-Ort Konfigurationen des Gerätes. Die Rolle *Maintenance* hat folgende Berechtigungen: Firmware Update, Auslesen von Logfiles, Konfigurationen des Gerätes (z.B. Setzen der Uhrzeit).	Handheld Terminal / Techniker Gerät	Wartungs-schnittstelle

Zentrales System Read-Only	Die Rolle *Read-Only* hat Lesezugriff auf definierte Speicherbereiche (z.B. Konfigurationseinstellungen oder Logfiles).	Zentrales System	WAN
Zentrales System Read-Write	Die Rolle *Read-Write* hat Zugriff auf alle Speicherbereiche und Funktionen. Die Rolle kann Privilegien allen Rollen ändern.	Zentrales System	WAN

B.3.3 Rollen am Zentralen System

Für eine rollen-basierte Zugangskontrolle werden Rollen und dazugehörige Privilegien sowie deren Anwendungsbereiche in der Architektur definiert. Hierbei sind lediglich die minimal zu unterstützenden Rollen der in der Architektur definierten Komponenten beschrieben. Bei den dargestellten Privilegien handelt es sich um Vorschläge. Die konkrete Ausprägung ist vom Netzbetreiber festzulegen.

Rollen am Head-End System

Rollen-bezeichnung	Privilegien	Anwendungs-bereich	Schnittstellen am Zentralen System
Head-End Maintenance	Die Rolle Head-End Maintenance kann das Head-End konfigurieren.	Head-End	Benutzer-schnittstelle
MDMS	Diese Rolle erlaubt dem MDMS, sich dem Head-End gegenüber zu authentifizieren.	Head-End	MDM_HE
Operator Read-Only	Diese Rolle erlaubt dem Benutzer des Head-End Systems, Daten am Zähler oder Gateway auszulesen.	Head-End	Benutzer-schnittstelle
Operator Read-Write	Diese Rolle erlaubt dem Benutzer des Head-End Systems, Daten auf den Zähler oder das Gateway zu schreiben.	Head-End	Benutzer-schnittstelle

Rollen am MDMS

Rollen-bezeichnung	Privilegien	Anwendungs-bereich	Schnittstellen am Zentralen System
Head-End	Erlaubt es dem Head-End System, sich gegenüber dem MDMS zu authentifizieren.	MDMS	MDM_HE
MDMS Maintenance	Die Rolle MDMS Maintenance kann das MDMS konfigurieren, und insbesondere definieren, welche Daten vom MDMS zum Kundenportal und das Back-End System weitergeleitet werden.	MDMS	Benutzer-schnittstelle
Operator Read-Only	Diese Rolle erlaubt dem Benutzer des MDMS, Daten auszulesen.	MDMS	Benutzer-schnittstelle
Operator Read-Write	Diese Rolle erlaubt dem Benutzer des MDMS Daten zu schreiben.	MDMS	Benutzer-schnittstelle

Rollen am Kundenportal

Rollen-bezeichnung	Privilegien	Anwendungs-bereich	Schnittstellen am Zentralen System
Kunde	Die Rolle Kunde kann auf einen oder mehrere Datensätze im Kundenportal zugreifen. Jedem Kunden und Drittanbieter wird hierbei eine individuelle Rolle zugewiesen.	Kundenportal	Internet
Kundenportal Maintenance	Konfiguriert das Kundenportal.	Kundenportal	Benutzer-schnittstelle

MDMS_KP	Erlaubt dem MDMS, sich dem Kundenportal gegenüber zu authentifizieren.	Kundenportal	MDM_KP

Rollen am Key Management System

Rollen-bezeichnung	Privilegien	Anwendungs-bereich	Schnittstellen am Zentralen System
KMS Maintenance	Die Rolle KMS Maintenance konfiguriert das Key Management System.	Key Management System	Benutzer-schnittstelle
Kundenportal	Erlaubt es dem Kundenportal, sich dem Key Management System gegenüber zu authentifizieren.	Key Management System	KP_KMS
Head-End	Erlaubt es dem Head-End, sich gegenüber dem Key Management System zu authentifizieren.	Key Management System	HE_KMS
MDMS	Erlaubt es dem MDMS, sich gegenüber dem Key Management System zu authentifizieren.	Key Management System	MDM_KMS

B.4 Sicherheitsereignisse

Für ein sicherheitsrelevantes Ereignis soll soweit möglich Zeit, Kennung (ID) des verursachenden Benutzers bzw. Systems, Schnittstelle, sowie das Ergebnis der Aktion protokolliert werden.

Zähler und Gateway sollen mindestens die folgenden Ereignis-Typen unterstützen:

Ereignis	Gerät
Registrieren einer erfolgreichen oder fehlgeschlagenen Authentifizierung für eine bestimmte Rolle.	Zähler und Gateway
Durchführung eines Firmware-Updates. • Protokollieren von erfolgreichen Firmware-Updates. • Protokollieren von fehlgeschlagenen Firmware-Updates aufgrund einer ungültigen Signatur.	Zähler und Gateway

• Unterscheidung zwischen dem Empfangen einer Firmware und der Aktivierung eines Firmware-Updates.	
Setzen der Systemzeit.	Zähler und Gateway
Ereignisse welche durch die Manipulationssensoren registriert werden. Hierzu zählen zum Beispiel das Öffnen von Gehäusedeckeln.	Zähler und Gateway
Starten eines Gerätes (Bootvorgang).	Zähler und Gateway
Durchführen eines Reset oder Reboots des Gerätes.	Zähler und Gateway
Rücksetzen von Fehler- oder Ereignisregistern oder den zugehörigen Protokollen.	Zähler und Gateway
Registrieren von Gerätefehlern. Siehe Anforderungen SRR_02.*	Zähler und Gateway
Rekonfiguration von kryptografischen Parametern. Zum Beispiel: • Aktualisierung von Schlüsselmaterial für eine bestimmte Rolle • Ändern von Zugriffsberechtigungen für eine bestimmte Rolle • Neuinitialisierung des Zufallszahlengenerators	Zähler und Gateway
Schalten des Breaker: aus / einschaltbereit.	Zähler
Ereignisse im Bezug auf Spartenzähler: • Durchführen eines Gerätepairings zwischen Sparten- und Stromzähler • Aktualisierung von Schlüsselmaterial für einen Spartenzähler	Zähler
Änderung der Parameter der Leistungsgrenze	Zähler
Leistungsbegrenzung	Zähler

C. Sicherheit der Zählerkommunikation

C.1 Allgemeine Sicherheitsanforderungen

C.1.1 Zukunftssicherheit

Anf._ID	
SFR_01.ZL	**Anforderung**
	Der Zähler MUSS genügend Reserven an Speicherplatz (flüchtiger und nicht-flüchtiger Speicher) und Rechenleistung aufweisen, um die Aktualisierung der Sicherheitsfunktionalität zu gewährleisten. Die Aktualisierbarkeit MUSS für den Produktlebenszyklus gewährleistet sein.
	Empfehlung und Umsetzungserläuterungen
	1. Der Hersteller SOLL in entsprechenden Designunterlagen nachweisen, dass hinreichende Reserven im Zähler vorhanden sind, um die Sicherheitsfunktionalität zu aktualisieren. 2. Hierbei sind insbesondere kryptografischen Algorithmen und Kommunikationsprotokolle betroffen. Es ist Anforderung SPR_01 beachten. 3. Der Zähler SOLL über einen reservierten Speicherbereich verfügen, der ausschließlich für Aktualisierungen der Sicherheitsfunktionalität verwendet werden darf.
	Empfohlene Qualitätssicherungsmaßnahme
	1. Die Analyse der Designinformationen des Herstellers wird empfohlen.
SFR_01.GW	**Anforderung**
	Das Gateway MUSS genügend Reserven an Speicherplatz (flüchtiger und nicht-flüchtiger Speicher) und Rechenleistung aufweisen, um die Aktualisierung der Sicherheitsfunktionalität zu gewährleisten. Die Aktualisierbarkeit MUSS für den Produktlebenszyklus gewährleistet sein.
	Empfehlung und Umsetzungserläuterungen

	1. Der Hersteller SOLL in entsprechenden Designunterlagen nachweisen, dass hinreichende Reserven im Gateway vorhanden sind, um die Sicherheitsfunktionalität zu aktualisieren. 2. Hierbei sind insbesondere kryptografischen Algorithmen und Kommunikationsprotokolle betroffen. Es ist Anforderung SPR_01 beachten. 3. Das Gateway SOLL über einen reservierten Speicherbereich verfügen, der ausschließlich für Aktualisierungen der Sicherheitsfunktionalität verwendet werden darf.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Analyse der Designinformationen des Herstellers wird empfohlen.
SFR_01.ZS	**Anforderung**
	Das Zentrale System MUSS die Aktualisierung der Sicherheitsfunktionalität unterstützen. Die Aktualisierbarkeit MUSS für den Produktlebenszyklus gewährleistet sein.
	Empfehlung und Umsetzungserläuterungen
	1. Der Hersteller SOLL in entsprechenden Designunterlagen nachweisen, dass es möglich ist die Sicherheitsfunktionalität zu aktualisieren. 2. Hierbei sind insbesondere kryptografischen Algorithmen und Kommunikationsprotokolle betroffen. Es ist Anforderung SPR_01 beachten.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Analyse der Designinformationen des Herstellers wird empfohlen.
SFR_02.ZL	**Anforderung**
	Aktualisierungen der kryptografischen Algorithmen und Kommunikationsprotokolle des Zählers MÜSSEN über Fernzugriff als Firmware-Update durchgeführt werden.

	Empfehlung und Umsetzungserläuterungen
	1. Es ist Anforderung SPR_01 beachten. 2. Die Aktualisierung des Zählers per Fernzugriff SOLL per Remote Firmware Update oder Remote Patching erfolgen.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Analyse der Designinformationen des Herstellers wird empfohlen. 2. Durchführung von Fuzzing Tests der betreffenden Firmware-Update Funktionen.
SFR_02.GW	**Anforderung**
	Aktualisierungen der kryptografischen Algorithmen und Kommunikationsprotokolle des Gateways MÜSSEN über Fernzugriff als Firmware-Update durchgeführt werden.
	Empfehlung und Umsetzungserläuterungen
	1. Es ist Anforderung SPR_01 beachten. 2. Die Aktualisierung des Gateways per Fernzugriff SOLL per Remote Firmware Update oder Remote Patching erfolgen.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Analyse der Designinformationen des Herstellers wird empfohlen. 2. Durchführung von Fuzzing Tests der betreffenden Firmware-Update Funktionen.
SFR_03.ZL	**Anforderung**
	Der Zähler MUSS sowohl die Widerrufung als auch die Aktualisierung aller Berechtigungen der jeweiligen Rollen und jegliches kryptografischen Schlüsselmaterials im Fernbetrieb unterstützen.
	Empfehlung und Umsetzungserläuterungen

	1. Siehe auch Anforderungen zur ZugangskontrolleZugangskontrolle im Kapitel C.4. 2. Um die Integrität des kryptografischen Schlüsselmaterials zu gewährleisten SOLL ein authentifizierter Schlüsselaustauschmechanismus implementiert werden. 3. Bei Anwendung von Public-Key Verfahren SOLL der Zähler neue Schlüsselpaare (öffentlich/privat) zusammen mit einer Zertifikatsanforderung (certificate signing request) erzeugen sowie neue Zertifikate importieren können. 4. Die Anforderung gilt auch für die Aktualisierbarkeit von öffentlichen Schlüsselmaterial, welches für die Validierung der digital signierten Firmware-Updates genutzt wird.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Test der implementierten Funktionen zur Verifizierung der Anforderung.
SFR_03.GW	**Anforderung**
	Das Gateway MUSS sowohl die Widerrufung als auch die Aktualisierung der Berechtigungen der jeweiligen Rollen und des kryptografischen Schlüsselmaterials im Fernbetrieb unterstützen.
	Empfehlung und Umsetzungserläuterungen
	1. Siehe auch Anforderungen zur ZugangskontrolleZugangskontrolle im Kapitel C.4. 2. Um die Integrität des kryptografischen Schlüsselmaterials zu gewährleisten SOLL ein authentifizierter Schlüsselaustauschmechanismus implementiert werden. 3. Bei Anwendung von Public-Key Verfahren SOLL das Gateway neue Schlüsselpaare (öffentlich/privat) zusammen mit einer Zertifikatsanforderung (certificate signing request) erzeugen sowie neue Zertifikate importieren können.
	Empfohlene Qualitätssicherungsmaßnahmen

	1. Test der implementierten Funktionen zur Verifizierung der Anforderung.
SFR_03.ZS	**Anforderung**
	Das Zentrale System MUSS sowohl die Widerrufung als auch die Aktualisierung der Berechtigungen der jeweiligen Rollen und des kryptografischen Schlüsselmaterials unterstützen.
	Empfehlung und Umsetzungserläuterungen
	1. Siehe auch Anforderungen zur Zugangskontrolle~~Zugangskontrolle~~ im Kapitel C.4. 2. Um die Integrität des kryptografischen Schlüsselmaterials zu gewährleisten ist Anforderung SIR_01C zu beachten.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Test der implementierten Funktionen zur Verifizierung der Anforderung.

C.1.2 Schnittstellen-Reduzierung

Anf._ID	
SMR_01	**Anforderung**
	Jede Schnittstelle DARF NUR die zur Systemfunktionalität benötigten Datentypen und Kommunikationsprotokolle unterstützen.
	Empfehlung und Umsetzungserläuterungen
	1. Der Hersteller SOLL anhand einer Design-Dokumentation in hinreichender Detailtiefe nachweisen, dass nur die benötigte Funktionalität implementiert ist. 2. Der Hersteller SOLL ein vollständiges Verzeichnis der unterstützten Datentypen und Kommunikationsprotokolle nachweisen. 3. Ein Beispiel für nicht benötigte Funktionen stellen Analysefunktionen des Herstellers dar, welche während des Entwicklungsprozesses genutzt wurden. Hierzu zählen zum Beispiel ein Webserver auf dem Gateway, der

	während der Entwicklung für Debugfunktionen verwendet wurde, sowie spezielle Tastenkombinationen zum Erreichen eines Engineering Menüs, welches sicherheitsrelevante Änderungen erlaubt.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung von Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung hinreichend implementiert wurde.
SMR_02	**Anforderung**
	Abgeschaltete oder unbenutzte Systemfunktionalität DARF die Sicherheitsfunktionen NICHT kompromittieren.
	Empfehlung und Umsetzungserläuterungen
	1. Der Hersteller SOLL eine Design-Dokumentation in hinreichender Detailtiefe liefern, die belegt, dass die Sicherheit des Systems nicht durch Funktionen beeinträchtigt wird, die über den normalen Zählerbetrieb oder die Kommunikation von Zähler und dem Zentralen System hinausgehen. 2. Abgeschaltete Funktionen, die auch in zukünftigen Anwendungen unbenutzt bleiben, SOLLEN vollständig entfernt werden. 3. Abgeschaltete Funktionen SOLLEN weder über weitere nicht dokumentierte Funktionen noch über undefinierte bzw. fehlerhafte Betriebszustände ansprechbar sein. o Ein Beispiel für unbenutzte Funktionalität, die auch in zukünftigen Anwendungen unbrauchbar bleiben, stellen nicht verwendete Firmware-Routinen dar, welche im Normalbetrieb nicht aufgerufen werden können, aber in der Firmware implementiert sind. o Weitere Beispiele sind Funktionen zum Testen, Debuggen oder zur Initialisierung im Rahmen des Produktionsprozesses.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung von Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung hinreichend implementiert wurde. 2. Ein Nachweis für die Durchführung eines Softwarereviews von Seiten des Herstellers.

C.1.3 Kryptografische Algorithmen

Anf._ID	
SPR_01	**Anforderung**
	1. Der Hersteller MUSS sich bei der Verwendung von kryptografischen Verfahren und Primitiven sowie Schlüssellängen an die jeweils aktuelle Fassung einer der folgenden beiden Richtlinien halten: • NIST SP 800-57, Recommendation for Key Management – Part 1: General (Revision 4). [4] • BSI TR-03116, Teil 3 „Kryptographische Vorgaben für Projekte der Bundesregierung – Intelligente Messsysteme“. In der in [5] referenzierten Version von 2017 finden nur die Kapitel 2 „Kryptographische Algorithmen“ und Kapitel 4.2 „Cipher Suites und Kurvenparameter“ Anwendung.[2] 2. Das Verwenden von proprietären kryptografischen Verfahren und Primitiven sowie das Abändern der in Punkt 1 genannten Verfahren ist ausgeschlossen.
	Empfehlung und Umsetzungserläuterungen
	1. Die TR-03116-3 wird jährlich aktualisiert und an die technischen und wissenschaftlichen Erkenntnisse angepasst. Ebenso ist auf Aktualisierungen von NIST SP 800-57 Part 3 zu achten. 2. Vorgaben zum Stand der Technik in der Kryptografie sind unter anderem in der BSI TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ [6] zu finden. 3. Die folgenden Algorithmen und Verfahren werden empfohlen. Erläuterungen zu den Bezeichnungen sind in den Richtlinien [5] und [4] zu finden: • Symmetrische Verfahren mit Authentifizierung: AES-CBC-CMAC, AES-CCM, AES-GCM. Bei der Implementierung von AES-GCM ist der Anhang (Appendix) in NIST SP 800-38D [7] zu beachten.

[2] Insbesondere sind die BSI Vorgaben für ein TLS-gesichertes HAN nicht Teil der hier definierten Zählerarchitektur.

	• Kryptografische Hashfunktionen: SHA2 Familie. • Authentifizierte Schlüsselaushandlung mit Elliptic Curve Diffie-Hellman (ECKA-DH). • Authentifizierter Schlüsseltransport mit Elliptic Curve El-Gamal (ECKA-EG). • Digitale Signaturen: ECDSA. • EC Verfahren SOLLEN elliptische Kurven über Primkörpern mit einer Länge von minimal 256 Bits wie z.B. die NIST Kurven (P-256 oder höhere Sicherheit) in IETF RFC 5114 [8] oder Kurven aus ECC Brainpool [9] verwenden. 4. Für die Kommunikation auf der WAN-Schnittstelle zwischen dem Zentralen System und dem Gateway sowie innerhalb des Zentralen Systems SOLL zusätzlich das TLS Protokoll in der Version 1.2 [10] (oder höher) unterstützt werden. Hierbei SOLL eine der folgenden Cipher Suites [11] verwendet werden: • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 5. Der Hersteller SOLL die Einhaltung dieser Anforderung anhand einer Design-Dokumentation in hinreichender Detailtiefe nachweisen. 6. Im Hinblick auf erforderlichen Speicher und Aktualisierungen der kryptografischen Funktionen siehe auch Anforderungen SFR_01.*. 7. Bei der Verwendung von Zertifikaten SOLL eine vertrauenswürdige Zeit bzw. Zeitquelle auf den genutzten Systemen/Geräten gewährleistet sein.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Verifikation der Anforderung erfolgt durch einen Test der implementierten Funktionen. 2. Die Analyse der Designinformationen des Herstellers wird empfohlen.
SPR_02	**Anforderung**
	Alle sicherheitsrelevanten Zufallswerte MÜSSEN durch kryptografische Zufallszahlengeneratoren gemäß AIS 20 [15] oder AIS 31 [16] oder äquivalent erzeugt werden.

	Empfehlung und Umsetzungserläuterungen
	1. Der Hersteller SOLL die Einhaltung dieser Anforderung anhand einer Design-Dokumentation in hinreichender Detailtiefe nachweisen. 2. Sicherheitsrelevante Zufallswerte werden unter anderem bei der Erstellung von Signaturen, Erzeugen von kryptografischem Schlüsselmaterial oder bei gegenseitiger Authentifizierung verwendet. 3. Die Dokumente FIPS 186-2 [12] und FIPS 140-2 (Annex C) [14] können als äquivalent erachtet werden.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung von Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung hinreichend implementiert wurde. 2. Die Analyse der Designinformationen des Herstellers wird empfohlen.
SPR_03	**Anforderung**
	Die verwendeten kryptografischen Algorithmen MÜSSEN einer Modul-Validierung gemäß NIST Cryptographic Algorithm Validation Program (CAVP) [17] oder äquivalenten Test- und Abnahmebedingungen unterworfen werden.
	Empfehlung und Umsetzungserläuterungen
	1. Äquivalente Test- und Abnahmebedingungen können auch von einer vom Regulator noch zu benennen Prüfstelle in Österreich vorgegeben werden. 2. Der Hersteller SOLL die Einhaltung dieser Anforderung anhand einer Design-Dokumentation in hinreichender Detailtiefe nachweisen, bzw. den Nachweis der Modul-Validierung oder dessen Äquivalenz erbringen.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Verifikation der Anforderung erfolgt durch eine Modul-Validierung der implementierten Funktionen oder Begutachtung der durchgeführten Modul-Validierung.

C.2 Datenintegrität

Anf._ID	
SIR_01.ZL	**Anforderung**
	Der Zähler MUSS die Authentizität und Integrität der übermittelten Daten an den folgenden Schnittstellen verifizieren: • Multi-Utility-Schnittstelle zwischen Stromzähler und Spartenzähler, • Wartungsschnittstelle, • LAN zwischen Stromzähler und Zentralem System, • WAN zwischen Stromzähler und Zentralem System. Bei der Überprüfung MÜSSEN sowohl die Quelle als auch die Authentizität der Nachricht selbst überprüft werden. Falls die Authentizität des Senders oder der Daten nicht verifiziert werden kann, MÜSSEN die Daten verworfen werden.
	Empfehlung und Umsetzungserläuterungen
	1. Die Authentizität der Nachricht SOLL durch das Anhängen eines Nachrichtenauthentifizierungscodes (MAC) gewährleistet werden. 2. Die Authentizität des Senders kann durch das Verifizieren einer angehängten validen digitalen Signatur bestätigt werden. 3. Die zulässigen kryptografischen Algorithmen sind in Anforderung SPR_01 zu finden. 4. In der Ende-zu-Ende Sicherheitsarchitektur bezieht sich diese Anforderung auf die Anwendungsschicht (OSI-Layer 5-7).
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Der Hersteller kann anhand einer Design-Dokumentation in hinreichender Detailtiefe nachweisen, dass die benötigten Funktionen implementiert sind. 2. Die Durchführung von Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung hinreichend implementiert wurde.
SIR_01.GW	**Anforderung**

	Das Gateway MUSS die Authentizität und Integrität der übermittelten Daten an den folgenden Schnittstellen verifizieren: • Wartungsschnittstelle, • WAN-Schnittstelle zum Zentralen System, wenn diese für Wartungszwecke des Gateways über das Zentrale System genutzt wird. Bei der Überprüfung MÜSSEN sowohl die Quelle als auch die Authentizität der Nachricht selbst überprüft werden. Falls die Authentizität des Senders oder der Daten nicht verifiziert werden kann, MÜSSEN die Daten verworfen werden.
	Empfehlung und Umsetzungserläuterungen
	1. Die Authentizität der Nachricht SOLL durch das Anhängen eines Nachrichtenauthentifizierungscodes (MAC) gewährleistet werden. 2. Die Authentizität des Senders kann durch das Verifizieren einer angehängten validen digitalen Signatur bestätigt werden. 3. Die zulässigen kryptografischen Algorithmen sind in Anforderung SPR_01 zu finden. 4. In der Ende-zu-Ende Sicherheitsarchitektur bezieht sich diese Anforderung auf die Anwendungsschicht (OSI-Layer 5-7).
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Der Hersteller kann anhand einer Design-Dokumentation in hinreichender Detailtiefe nachweisen, dass die benötigten Funktionen implementiert sind. 2. Die Durchführung von Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung hinreichend implementiert wurde.
SIR_01.ZS	**Anforderung**
	Das Zentrale System MUSS die Authentizität und Integrität der Daten an allen Schnittstellen sowie beim Datenverkehr zwischen den implementierten Zonen verifizieren. Bei der Überprüfung MÜSSEN sowohl die Quelle als auch die Authentizität der Nachricht selbst überprüft werden. Falls die Authentizität des Senders oder der Daten nicht verifiziert werden

	kann, MÜSSEN die Daten verworfen werden.
	Empfehlung und Umsetzungserläuterungen
	1. Zonen im Zentralen System sind in Anforderung SRR_04.ZS näher beschrieben. 2. Die Authentizität der Nachricht SOLL durch das Anhängen eines Nachrichtenauthentifizierungscodes (MAC) gewährleistet werden. 3. Die Authentizität des Senders kann durch das Verifizieren einer angehängten validen digitalen Signatur bestätigt werden. 4. Die zulässigen kryptografischen Algorithmen sind in Anforderung SPR_01 zu finden. 5. In der Ende-zu-Ende Sicherheitsarchitektur bezieht sich diese Anforderung auf die Anwendungsschicht (OSI-Layer 5-7).
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Der Hersteller kann anhand einer Design-Dokumentation in hinreichender Detailtiefe nachweisen, dass die benötigten Funktionen implementiert sind. 2. Die Durchführung von Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung hinreichend implementiert wurde.
SIR_02.ZL	**Anforderung**
	Der Zähler MUSS die Validität der empfangenen Datenpakete sowie des Datenformats an den folgenden Schnittstellen verifizieren: • Multi-Utility-Schnittstelle zwischen Stromzähler und Spartenzähler, • Wartungsschnittstelle, • LAN zwischen Stromzähler und Zentralem System, • WAN zwischen Stromzähler und Zentralem System.
	Empfehlung und Umsetzungserläuterungen
	1. Das Gerätedesign und die Implementierung SOLLEN gewährleisten, dass die korrekte Arbeitsweise des Zählers nicht von korrumpierten oder fehlerhaft formatierten Nachrichten negativ beeinträchtigt wird. 2. Die Anforderung bezieht sich sowohl auf die oberen als auch unteren

	Schichten im OSI-Modell.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Durchführung von Fuzzing Tests der betreffenden Schnittstellen. 2. Der Hersteller sollte die Sicherheitstests in einer für eine Bewertung hinreichende Detailtiefe dokumentieren und der Produktdokumentation hinzufügen.
SIR_02.GW	**Anforderung**
	Das Gateway MUSS die Validität der Datenpakete sowie des Datenformats an den folgenden Schnittstellen verifizieren: • Wartungsschnittstelle, • WAN-Schnittstelle, wenn diese für Wartungszwecke des Gateways über das Zentrale System genutzt wird.
	Empfehlung und Umsetzungserläuterungen
	1. Das Gerätedesign und die Implementierung SOLLEN gewährleisten, dass die korrekte Arbeitsweise des Gateways nicht von korrumpierten oder fehlerhaft formatierten Nachrichten negativ beeinträchtigt wird. 2. Die Anforderung bezieht sich sowohl auf die oberen als auch unteren Schichten im OSI-Modell.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Durchführung von Fuzzing Tests der betreffenden Schnittstellen. 2. Der Hersteller sollte die Sicherheitstests in einer für eine Bewertung hinreichende Detailtiefe dokumentieren und der Produktdokumentation hinzufügen.
SIR_02.ZS	**Anforderung**
	Das Zentrale System MUSS die Validität der Datenpakete sowie des Datenformats an allen Schnittstellen sowie beim Datenverkehr zwischen den implementierten Zonen verifizieren.

	Empfehlung und Umsetzungserläuterungen
	1. Zonen im Zentralen System sind in Anforderung SRR_04.ZS näher beschrieben. 2. Die Anforderung betrifft sowohl die externen als auch die internen (von Zone zu Zone) Schnittstellen des Zentralen Systems. 3. Das Design und die Implementierung SOLLEN gewährleisten, dass die korrekte Arbeitsweise des Zentralen Systems nicht von korrumpierten oder fehlerhaft formatierten Nachrichten negativ beeinträchtigt wird. 4. *SQL Bereinigung* ist eine Gegenmaßnahme zu *SQL Einschleusung* (SQL injection) und stellt ein Beispiel für die Validierung von Datenpaketen im Zentralen System dar. Mehr Beispiele zu Validierung von Datenpaketen bei Webservern sind in der ÖNORM A 7700 [18] und im Kapitel „*Datenvalidierung“ der OWASP Gruppe* [19] beschrieben. 5. Die Anforderung bezieht sich sowohl auf die oberen als auch unteren Schichten im OSI-Modell.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Durchführung von Fuzzing Tests der betreffenden Schnittstellen. 2. Der Hersteller sollte die Sicherheitstests in einer für eine Bewertung hinreichende Detailtiefe dokumentieren und der Produktdokumentation hinzufügen.
SIR_03.ZL	**Anforderung**
	Der Zähler MUSS die Integrität von Firmware-Updates vor der Aktivierung verifizieren. • Der Hersteller MUSS das Firmware-Update digital signieren. • Firmware-Updates ohne gültige digitale Signatur MÜSSEN verworfen werden. • Falls die Versionsnummer des Firmware-Updates niedriger ist als die der installierten Firmware, MUSS das Firmware-Update verworfen werden. • Das Zähler MUSS, falls dies aus betrieblichen Gründen erforderlich ist, einen sicheren Rückstieg auf eine ältere Firmware Version ermöglichen. Ein solcher Rückstieg erfolgt durch das Einspielen der alten Firmware unter einer neuen Versionsnummer. • Die Gerätedaten (z.B. gespeicherte Messdaten, Protokolleinträge oder

	kundenspezifische Konfigurationen) DÜRFEN durch ein Update der Firmware NICHT verändert oder gelöscht werden. • Zwingend notwendige Änderungen an der Konfiguration von neuen oder geänderten Funktionen MÜSSEN während des Updateprozesses automatisch vorgenommen werden.
	Empfehlung und Umsetzungserläuterungen
	1. Der ECDSA Algorithmus mit einer zugelassenen Schlüssellänge SOLL zur Erstellung der digitalen Signatur verwendet werden. Siehe hierzu auch SPR_01. 2. Der öffentliche Schlüssel für die Validierung der digitalen Signatur SOLL während des Herstellungsprozesses auf den Zähler gespielt werden. Siehe hierzu Beispielprozesse in Anhang A. 3. Die Verwendung von digital signierten Firmware-Updates ermöglicht Broadcasts bzw. Multicasts. Siehe hierzu Beispielprozesse in Anhang A. 4. Der Freigabeprozess von Firmware-Updates beim Hersteller SOLL entsprechend gesichert und verwaltet sein, um ein vertrauenswürdiges Update zu gewährleisten.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Verifikation der funktionalen Anforderung erfolgt durch einen Test der implementierten Firmware-Update Funktionen. 2. Bezüglich der Anforderungen an die Prozesse können im Rahmen von Abnahme- und Funktionsprüfungen Sicherheitsprüfungen durchgeführt werden. 3. Sicherheitsüberprüfungen von Entwicklungs- und Freigabeprozessen können auch im Rahmen einer allgemeinen Auditierung z.B. von ISO27001 durchgeführt werden. 4. Durchführung von Fuzzing Tests der betreffenden Firmware-Update Funktionen.
SIR_03.GW	**Anforderung**
	Das Gateway MUSS die Integrität von Firmware-Updates vor der Aktivierung verifizieren. • Der Hersteller MUSS das Firmware-Update digital signieren.

	• Firmware-Updates ohne gültige digitale Signatur MÜSSEN verworfen werden. • Falls die Versionsnummer des Firmware-Updates niedriger ist als die der installierten Firmware, MUSS das Firmware-Update verworfen werden. • Das Gateway MUSS, falls dies aus betrieblichen Gründen erforderlich ist, einen sicheren Rückstieg auf eine ältere Firmware Version ermöglichen. Ein solcher Rückstieg erfolgt durch das Einspielen der alten Firmware unter einer neuen Versionsnummer. • Die Gerätedaten (z.B. Protokolleinträge) DÜRFEN durch ein Update der Firmware NICHT verändert oder gelöscht werden. Zwingend notwendige Änderungen an der Konfiguration von neuen oder geänderten Funktionen MÜSSEN während des Updateprozesses automatisch vorgenommen werden.
	Empfehlung und Umsetzungserläuterungen
	1. Der ECDSA Algorithmus mit einer zugelassenen Schlüssellänge SOLL zur Erstellung der digitalen Signatur verwendet werden. Siehe hierzu auch SPR_01. 2. Der öffentliche Schlüssel für die Validierung der digitalen Signatur SOLL während des Herstellungsprozesses auf das Gateway gespielt werden. Siehe hierzu Beispielprozesse in Anhang A. 3. Die Verwendung von digital signierten Firmware-Updates ermöglicht Broadcasts bzw. Multicasts. Siehe hierzu Beispielprozesse in Anhang A. 4. Der Freigabeprozess von Firmware-Updates beim Hersteller SOLL entsprechend gesichert und verwaltet sein, um ein vertrauenswürdiges Update zu gewährleisten.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Verifikation der funktionalen Anforderung erfolgt durch einen Test der implementierten Firmware-Update Funktionen. 2. Bezüglich der Anforderungen an die Prozesse können im Rahmen von Abnahme- und Funktionsprüfungen Sicherheitsprüfungen durchgeführt werden. 3. Sicherheitsüberprüfungen von Entwicklungs- und Freigabeprozessen können auch im Rahmen einer allgemeinen Auditierung z.B. von

	ISO27001 durchgeführt werden. 4. Durchführung von Fuzzing Tests der betreffenden Firmware-Update Funktionen.
SIR_03.ZS	**Anforderung**
	Das Zentrale System MUSS die Integrität von Software-Updates vor der Aktivierung verifizieren. • Der Hersteller MUSS das Software-Update digital signieren. • Software-Updates ohne gültige digitale Signatur MÜSSEN verworfen werden. • Das Zentrale System MUSS, falls dies aus betrieblichen Gründen erforderlich ist, einen sicheren Rückstieg auf eine ältere Software Version ermöglichen.
	Empfehlung und Umsetzungserläuterungen
	1. Der ECDSA Algorithmus mit einer zugelassenen Schlüssellänge SOLL zur Erstellung der digitalen Signatur verwendet werden. Siehe hierzu auch SPR_01. 2. Der Freigabeprozess von Software-Updates beim Hersteller SOLL entsprechend gesichert und verwaltet sein, um ein vertrauenswürdiges Update zu gewährleisten.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Verifikation der funktionalen Anforderung erfolgt durch einen Test der implementierten Software-Update Funktionen. 2. Bezüglich der Anforderungen an die Prozesse können im Rahmen von Abnahme- und Funktionsprüfungen Sicherheitsprüfungen durchgeführt werden. 3. Sicherheitsüberprüfungen von Entwicklungs- und Freigabeprozessen können auch im Rahmen einer allgemeinen Auditierung z.B. von ISO27001 durchgeführt werden.

SIR_04.ZL	**Anforderung**
	Der Zähler MUSS Wiedereinspielung (replay) von Nachrichten an den folgenden Schnittstellen erkennen können: • Multi-Utility-Schnittstelle zwischen Stromzähler und Spartenzähler, • Wartungsschnittstelle, • LAN zwischen Stromzähler und Zentralem System, • WAN zwischen Stromzähler und Zentralem System. Eine wiedereingespielte Nachricht MUSS vom Zähler verworfen werden.
	Empfehlung und Umsetzungserläuterungen
	1. Um Wiedereinspielangriffe abzuwehren, SOLLEN alle Nachrichten wie folgt gesichert werden: • Zum Beispiel durch das Anhängen einer Nachrichtennummer (counter). • Zum Beispiel durch das Anhängen von authentifizierte Nonces (Nonce und MAC). Wichtig ist, dass die Nonce durch einen MAC authentifiziert ist. • Zum Beispiel durch Verschlüsselung mit anschließender Authentifizierung mit Verfahren wie zum Beispiel AES-CBC-CMAC, AES-CCM, AES-GCM.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung von Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung hinreichend implementiert wurde. 2. Die Analyse der Designinformationen des Herstellers wird empfohlen.
SIR_04.GW	**Anforderung**
	Das Gateway MUSS Wiedereinspielung (replay) von Nachrichten an den folgenden Schnittstellen erkennen können: • Wartungsschnittstelle, • WAN-Schnittstelle zum Zentralen System, wenn diese für Wartungszwecke des Gateways über das Zentrale System genutzt

	wird. Eine wiedereingespielte Nachricht MUSS vom Gateway verworfen werden.
	Empfehlung und Umsetzungserläuterungen
	1. Um Wiedereinspielangriffe abzuwehren, SOLLEN alle Nachrichten wie folgt gesichert werden: • Zum Beispiel durch das Anhängen einer Nachrichtennummer (counter). • Zum Beispiel durch das Anhängen von authentifizierte Nonces (Nonce und MAC). Wichtig ist, dass die Nonce durch einen MAC authentifiziert ist. • Zum Beispiel durch Verschlüsselung mit anschließender Authentifizierung mit Verfahren wie zum Beispiel AES-CBC-CMAC, AES-CCM, AES-GCM.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung von Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung hinreichend implementiert wurde. 2. Die Analyse der Designinformationen des Herstellers wird empfohlen.
SIR_04.ZS	**Anforderung**
	Das Zentrale System MUSS Wiedereinspielung (replay) von Nachrichten an allen externen und internen (Zone zu Zone) Schnittstellen erkennen können. Eine wiedereingespielte Nachricht MUSS verworfen werden.
	Empfehlung und Umsetzungserläuterungen
	1. Um Wiedereinspielangriffe abzuwehren, SOLLEN alle Nachrichten wie folgt gesichert werden: • Zum Beispiel durch das Anhängen einer Nachrichtennummer (counter). • Zum Beispiel durch das Anhängen von authentifizierte Nonces (Nonce und MAC). Wichtig ist dass die Nonce durch einen MAC

	authentifiziert ist. • Zum Beispiel durch Verschlüsselung mit anschließender Authentifizierung mit Verfahren wie zum Beispiel AES-CBC-CMAC, AES-CCM, AES-GCM. 2. Diese Funktionalität kann durch die Verwendung von TLS oder eines VPNs gewährleistet werden. Siehe dazu auch SPR_01.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung von Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung hinreichend implementiert wurde. 2. Die Analyse der Designinformationen des Herstellers wird empfohlen.

C.3 Lokale Sicherung

Anf._ID	
SRR_01.ZL	**Anforderung**
	Verschiedene funktionelle Blöcke des Zählers DÜRFEN einander NICHT beeinträchtigen. Funktionen, die nicht zur Sicherheit beitragen, DÜRFEN die Sicherheit des Gesamtsystems NICHT beeinträchtigen. Der Hersteller MUSS die Trennung von sicherheitsrelevanten und nicht-sicherheitsrelevanten Funktionen und Blöcken nachweisen.
	Empfehlung und Umsetzungserläuterungen
	1. Der Hersteller SOLL anhand einer Design-Dokumentation nachweisen, dass der Zähler hinreichend in funktionelle Blöcke partitioniert ist. 2. Ein Beispiel für die Trennung von funktionalen Blöcken ist die Trennung von Kommunikation und Metrologie am Zähler. Beispielsweise darf eine Beeinträchtigung der Kommunikation keine Beeinträchtigung der Metrologie nach sich ziehen.
	Empfohlene Qualitätssicherungsmaßnahmen

	1. Die Durchführung von Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung hinreichend implementiert wurde. 2. Die Durchführung von Fuzzing Tests wird empfohlen, um sicherzustellen, dass sich einzelne Funktionsblöcke des Zählers nicht gegenseitig beeinträchtigen.
SRR_01.GW	**Anforderung**
	Verschiedene funktionelle Blöcke des Gateways DÜRFEN einander NICHT beeinträchtigen. Funktionen, die nicht zur Sicherheit beitragen, DÜRFEN die Sicherheit des Gesamtsystems NICHT beeinträchtigen. Der Hersteller MUSS die Trennung von sicherheitsrelevanten und nicht-sicherheitsrelevanten Funktionen und Blöcken nachweisen.
	Empfehlung und Umsetzungserläuterungen
	1. Der Hersteller SOLL anhand einer Design-Dokumentation nachweisen, dass das Gateway hinreichend in funktionelle Blöcke partitioniert ist. 2. Ein Beispiel für die Trennung von funktionalen Blöcken im Gateway stellt Speicherschutz für verschiedene Prozesse (Routing, Fernzugriff) dar.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung von Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung hinreichend implementiert wurde. 2. Die Durchführung von Fuzzing Tests wird empfohlen, um sicherzustellen, dass sich einzelne Funktionsblöcke des Gateways nicht gegenseitig beeinträchtigen.
SRR_02.ZL	**Anforderung**
	Der Zähler MUSS *fail-secure* sein. • Bei Versagen oder Ausfall einer Gerätefunktion MÜSSEN die Vertraulichkeit und Integrität von Daten und Funktionen im Zähler

	weiterhin gewährleistet sein. • Der Zähler MUSS einen sicheren Zustand bewahren, auch wenn Fehler und unerwünschte bzw. nicht vorhergesehene Betriebszustände auftreten (zufällig oder mutwillig herbeigeführt). Relevante Fehlertypen und die getroffenen Schutzmaßnahmen MÜSSEN vom Hersteller angegeben werden.
	Empfehlung und Umsetzungserläuterungen
	1. Der Hersteller SOLL anhand einer Design-Dokumentation nachweisen, dass der Zähler fail-secure ist. 2. Ein solcher Nachweis SOLL durch die Implementierung einer Überwachungsfunktion (Watchdog) erbracht werden, die bei einer technischen Störung die Beibehaltung des gesicherten operativen Betriebs gewährleistet. 3. Beispiele für relevante Fehler sind: • Spannungsverlust • Integritätsfehler (beispielsweise von Einstellungen, Konfigurationsdaten, Protokolldateien) • Fehler beim Selbsttest des Stromzählers • Fehler beim Ausführen kryptografischer Funktionen • Fehler beim Überprüfen der Zugriffsberechtigungen • Fehler bei der Dateneingabe (falsche Datenformate, falsche Datenfeldlänge, ungültige Befehle, etc.) • Fehler bei der Bedienung der lokalen Eingabetasten (Tastenfolge zu schnell, mehrere Tasten gleichzeitig gedrückt, etc.) 4. Der Hersteller SOLL in den Designinformationen nachweisen, welche relevanten Fehler abgedeckt sind und wie diese getestet wurden.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung von Penetrationstests wird zur Sicherung der Designstabilität empfohlen. 2. Die Analyse der Designinformationen des Herstellers wird empfohlen.
SRR_02.GW	**Anforderung**
	Das Gateway MUSS *fail-secure* sein. • Bei Versagen oder Ausfall einer Gerätefunktion MÜSSEN die Vertraulichkeit und Integrität von Daten und Funktionen auf dem

	Gateway weiterhin gewährleistet sein. • Das Gateway MUSS einen sicheren Zustand bewahren, auch wenn Fehler und unerwünschte bzw. nicht vorhergesehene Betriebszustände auftreten (zufällig oder mutwillig herbeigeführt). Relevante Fehlertypen und die getroffenen Schutzmaßnahmen MÜSSEN vom Hersteller angegeben werden.
	Empfehlung und Umsetzungserläuterungen
	1. Der Hersteller SOLL anhand einer Design-Dokumentation nachweisen, dass das Gateway fail-secure ist. 2. Ein solcher Nachweis SOLL durch die Implementierung einer Überwachungsfunktion (Watchdog) erbracht werden, die bei einer technischen Störung die Beibehaltung des gesicherten operativen Betriebs gewährleistet. 3. Beispiele für relevante Fehler sind: • Spannungsverlust • Integritätsfehler (beispielsweise von Einstellungen, Konfigurationsdaten, Protokolldateien) • Fehler beim Selbsttest des Gateways • Fehler beim Ausführen kryptografischer Funktionen • Fehler beim Überprüfen der Zugriffsberechtigungen • Fehler bei der Dateneingabe (falsche Datenformate, falsche Datenfeldlänge, ungültige Befehle, etc.) • Fehler bei der Bedienung der lokalen Eingabetasten (Tastenfolge zu schnell, mehrere Tasten gleichzeitig gedrückt, etc.) 4. Der Hersteller SOLL in den Designinformationen nachweisen, welche relevanten Fehler abgedeckt sind und wie diese getestet wurden.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung von Penetrationstests wird zur Sicherung der Designstabilität empfohlen. 2. Die Analyse der Designinformationen des Herstellers wird empfohlen.
SRR_02.ZS	**Anforderung**
	Das Zentrale System MUSS *fail-secure* sein. • Bei Versagen oder Ausfall von Teilen des Zentralen Systems MÜSSEN die Vertraulichkeit und Integrität von Daten und Funktionen

	im Zentralen System weiterhin gewährleistet sein. • Das Zentrale System MUSS einen sicheren Zustand bewahren, auch wenn Fehler und unerwünschte bzw. nicht vorhergesehene Betriebszustände auftreten (zufällig oder mutwillig herbeigeführt). Relevante Fehlertypen und die getroffenen Schutzmaßnahmen MÜSSEN vom Hersteller angegeben werden.
	Empfehlung und Umsetzungserläuterungen
	1. Der Hersteller SOLL anhand einer Design-Dokumentation nachweisen, dass das Zentrale System fail-secure ist. 2. Beispiele für relevante Fehler sind: • Integritätsfehler (beispielsweise von Einstellungen, Konfigurationsdaten, Protokolldateien) • Fehler beim Ausführen kryptografischer Funktionen • Fehler beim Überprüfen der Zugriffsberechtigungen • Fehler bei der Dateneingabe (falsche Datenformate, falsche Datenfeldlänge, ungültige Befehle, etc.) 3. Der Hersteller SOLL in den Designinformationen nachweisen, welche relevanten Fehler abgedeckt sind und wie diese getestet wurden.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung von Penetrationstests wird zur Sicherung der Designstabilität empfohlen. 2. Die Analyse der Designinformationen des Herstellers wird empfohlen.
SRR_03.ZL	**Anforderung**
	Physikalische Manipulationen am Zähler MÜSSEN erkennbar sein. • Das Gehäuse MUSS angemessenen Schutz gegen Manipulation bieten. • Das Zählergehäuse MUSS, wo möglich, versiegelt werden. • Zusätzlich MUSS am Zähler die Öffnung des Klemmendeckels und des Gehäuses (separat) mittels geeigneter Maßnahmen (Kontakte, Sensoren) durch die Zählerelektronik erkannt und protokolliert werden. • Falls abnehmbare Gehäuseteile vorhanden sind, MUSS das Entfernen eines solchen Gehäuseteiles einen Eintrag im

	Sicherheitsprotokoll erzeugen. Ein unabhängiger Penetrationstest bezüglich der physikalischen Sicherheit des Zählers MUSS durchgeführt werden.
	Empfehlung und Umsetzungserläuterungen
	1. Siehe Anforderung SLR_01.ZL zur Definition des Sicherheitsprotokolls. 2. Der Hersteller SOLL anhand einer Design-Dokumentation in hinreichender Detailtiefe nachweisen, dass die Anforderungen hinreichend implementiert wurden. 3. Das Zählergehäuse sowie der Klemmendeckel SOLLEN plombiert bzw. versiegelt werden können. 4. Der Penetrationstests SOLL einen Zeitrahmen von mindestens 2 Wochen umfassen und von einem erfahrenen Tester durchgeführt werden.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Analyse der im Penetrationstest berichteten Schwachstellen.
SRR_03.GW	**Anforderung**
	Physikalische Manipulationen am Gateway MÜSSEN erkennbar sein. • Das Gehäuse MUSS angemessenen Schutz gegen Manipulation bieten. Falls abnehmbare Gehäuseteile vorhanden sind, MUSS das Entfernen eines solchen Gehäuseteiles einen Eintrag im Sicherheitsprotokoll erzeugen.
	Empfehlung und Umsetzungserläuterungen
	1. Siehe Anforderung SLR_01.GW zur Definition des Sicherheitsprotokolls. 2. Der Hersteller SOLL anhand einer Design-Dokumentation in hinreichender Detailtiefe nachweisen, dass die Anforderungen hinreichend implementiert wurden.

	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung von Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung hinreichend implementiert wurde.
SRR_04.ZS	**Anforderung**
	1. Das Zentrale System MUSS die Unterteilung in mindestens die folgenden vier Zonen unterstützen: a. Head-End System b. Key-Management System (KMS) c. Meter-Data-Management System (MDMS) d. Kundenportal 2. Es MUSS möglich sein, die Kommunikation zwischen den Zonen einzuschränken.
	Empfehlung und Umsetzungserläuterungen
	1. Allgemeine Beispiele für Maßnahmen zur Einschränkung der Zonen sind: • Firewalls: Eine Firewall kann gezielt den Informationsfluss zwischen zwei Komponenten regeln. Bei der Konfiguration ist Vorsicht geboten: durch die Flexibilität kann es auch leicht zu Fehlkonfigurationen kommen, die Angriffe ermöglichen. • Netzwerk-Gateways[3]: Ein Gateway legt fest, welche Komponenten miteinander kommunizieren können. • Datendioden: Eine Datendiode erlaubt den Datenfluss nur in eine Richtung. Da der dedizierte Empfänger keine Daten an den Sender schicken kann, kann auf diesem Weg kein Angriff erfolgen. Datendioden sind i.d.R. deutlich sicherer, aber auch unflexibler als Firewalls und Gateways. • Microkernels: Ein Microkernel, oder Hypervisor erlaubt es, Prozesse auf einer Hardwarekomponente sicher zu trennen. Dadurch ist es möglich, auch ohne Hardwareseparierung Zonen einzusetzen.

[3] In dieser Anforderung ist „Gateway“ im klassischen Sinne als Bindeglied zwischen Rechnernetzen zu verstehen.

	2. Wenn möglich sollte die Einschränkung außerhalb der Komponente selbst umgesetzt werden.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung von Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung hinreichend implementiert wurde.
SRR_05.ZS	**Anforderung**
	Es MUSS möglich sein, das Schlüsselmaterial in einer gesicherten Umgebung innerhalb des Key-Management Systems abzulegen. Die gesicherte Umgebung MUSS mindestens Level 3 in FIPS 140-2 [13] entsprechen.
	Empfehlung und Umsetzungserläuterungen
	1. Bei der Verwendung von kryptografischen Funktionen ist Anforderung SPR_01 beachten. 2. Kritische kryptografische Schlüssel SOLLEN niemals außerhalb dieser gesicherten Umgebung existieren. 3. Es SOLL möglich sein, innerhalb der gesicherten Umgebung kryptografische Schlüssel zu erzeugen. 4. Die Schnittstellen zur gesicherten Umgebung SOLLEN einen offenen Schnittstellen-Standard benutzen, beispielsweise PKCS #11 [20]. 5. Sämtliche Schnittstellen der gesicherten Umgebung SOLLEN vollständig dokumentiert werden. 6. Es SOLL möglich sein, den die Zugriffsintervalle auf die gesicherten Daten zu beschränken. 7. Es SOLL möglich sein, ausgewählte Schlüssel nach dem Vier-Augen Prinzip zu schützen.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Analyse der Herstellerinformationen und validieren der vom Hersteller

	bereitgestellten Zertifizierungen.
SRR_06.ZS	**Anforderung**
	Es MUSS möglich sein, Kunden- und Authentifizierungsdaten auf dem Kundenportal im Zentralen System abzusichern.
	Empfehlung und Umsetzungserläuterungen
	1. Um Passwortdatenbanken vor Angriffen zu schützen, SOLLEN Password-Hashing Verfahren wie PBKDF2 [21] (oder Verfahren mit höherer Sicherheit) verwendet werden. 2. Es SOLL möglich sein, das Kundenportal in einen Anwendungsserver und Webserver zu trennen. Dadurch können z.B. die Kundendaten auf dem leichter zu schützendem Anwendungsserver gespeichert werden.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung von Penetrationstests wird empfohlen, um sicherzustellen, dass die Anforderung hinreichend implementiert wurde. 2. Die Analyse der Designinformationen des Herstellers wird empfohlen.

C.4 Zugangskontrolle

Anf._ID	
SAR_01.ZL	**Anforderung**
	Der Zähler MUSS Mechanismen für rollenbasierte Zugangskontrolle zum Schutz vor unbefugten Zugriffen unterstützen. • Es MÜSSEN mindestens die Kapitel B.3 definierten Rollen unterstützt werden. • Die Berechtigungen der einzelnen Rollen MÜSSEN konfigurierbar sein. • Es MUSS möglich sein, individuelles kryptografisches Schlüsselmaterial für jede Rolle zu erzeugen bzw. zu aktualisieren. • Rollen MÜSSEN an Schnittstellen gebunden werden können.

	• Im Hinblick auf Zukunftssicherheit MUSS es möglich sein, weitere Rollen und deren Berechtigungen entweder per Fernzugriff oder per Firmware-Update zu implementieren. • Alle implementierten Rollen MÜSSEN per Fernzugriff individuell deaktivierbar sein.
	Empfehlung und Umsetzungserläuterungen
	1. Der Hersteller SOLL anhand einer Design-Dokumentation in hinreichender Detailtiefe nachweisen, dass die Anforderungen hinreichend implementiert wurden.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung einer Funktionsprüfung der entsprechenden rollenbasierten Zugangskontrolle wird empfohlen. Hierbei soll sichergestellt werden, dass bei der Implementierung jeder Rolle nur die notwendigen Rechte bereitgestellt wurden.
SAR_01.GW	**Anforderung**
	Das Gateway MUSS Mechanismen für rollenbasierte Zugangskontrolle zum Schutz vor unbefugten Zugriffen unterstützen. • Es MÜSSEN mindestens die Kapitel B.3 definierten Rollen unterstützt werden. • Die Berechtigungen der einzelnen Rollen MÜSSEN konfigurierbar sein. • Es MUSS möglich sein, individuelles kryptografisches Schlüsselmaterial für jede Rolle zu erzeugen bzw. zu aktualisieren. • Rollen MÜSSEN an Schnittstellen gebunden werden können. • Im Hinblick auf Zukunftssicherheit MUSS es möglich sein, weitere Rollen und deren Berechtigungen entweder per Fernzugriff oder per Firmware-Update zu implementieren. • Alle implementierten Rollen MÜSSEN per Fernzugriff individuell deaktivierbar sein.

	Empfehlung und Umsetzungserläuterungen
	1. Der Hersteller SOLL anhand einer Design-Dokumentation in hinreichender Detailtiefe nachweisen, dass die Anforderungen hinreichend implementiert wurden.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung einer Funktionsprüfung der entsprechenden rollenbasierten Zugangskontrolle wird empfohlen. Hierbei soll sichergestellt werden, dass bei der Implementierung jeder Rolle nur die notwendigen Rechte bereitgestellt wurden.
SAR_01.ZS	**Anforderung**
	Das Zentrale System MUSS Mechanismen für rollenbasierte Zugangskontrolle zum Schutz vor unbefugten Zugriffen unterstützen. • Es MÜSSEN mindestens die Kapitel B.3 definierten Rollen unterstützt werden. • Die Berechtigungen der einzelnen Rollen MÜSSEN konfigurierbar sein. • Es MUSS möglich sein, individuelles kryptografisches Schlüsselmaterial für jede Rolle zu erzeugen bzw. zu aktualisieren. • Rollen MÜSSEN an Schnittstellen gebunden werden können. • Im Hinblick auf Zukunftssicherheit MUSS es möglich sein, weitere Rollen zu implementieren. • Alle implementierten Rollen MÜSSEN individuell deaktivierbar sein.
	Empfehlung und Umsetzungserläuterungen
	1. Der Hersteller SOLL anhand einer Design-Dokumentation in hinreichender Detailtiefe nachweisen, dass die Anforderungen hinreichend implementiert wurden.

	2. Der Verbindung zwischen menschlicher Autorisierung (Passwörter, Smartcards) und den Rollen SOLL durch ein geeignetes System (z.B. LDAP) hergestellt werden 3. Es SOLL möglich sein, Rollen so zu definieren, dass ein Vier-Augen Prinzip implementiert werden kann.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung einer Funktionsprüfung der entsprechenden rollenbasierten Zugangskontrolle wird empfohlen. Hierbei soll sichergestellt werden, dass bei der Implementierung jeder Rolle nur die notwendigen Rechte bereitgestellt wurden.
SAR_02.ZL	**Anforderung**
	Der Zähler MUSS Funktionen zur Verhinderung und Erkennung von unbefugtem Zugang unterstützen.
	Empfehlung und Umsetzungserläuterungen
	1. Es SOLLEN Mechanismen implementiert werden, die den Versuch von unbefugtem Zugang erkennen und wo möglich im Sicherheitsprotokoll festhalten. Ein Beispiel wäre der Versuch, auf ein geschütztes Datenobjekt zuzugreifen, für welches keine Berechtigung existiert. 2. Der Hersteller SOLL anhand einer Design-Dokumentation in hinreichender Detailtiefe nachweisen, dass die Anforderungen hinreichend implementiert wurden.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung einer Funktionsprüfung der entsprechenden Mechanismen zur Erkennung von unbefugtem Zugang wird empfohlen.

	2. Die Durchführung von Penetrationstests wird empfohlen, um sicherzustellen, dass diese Designanforderung hinreichend implementiert wurde.
SAR_02.GW	**Anforderung**
	Das Gateway MUSS Funktionen zur Verhinderung und Erkennung von unbefugtem Zugang unterstützen.
	Empfehlung und Umsetzungserläuterungen
	1. Es SOLLEN Mechanismen implementiert werden, die den Versuch von unbefugtem Zugang erkennen und wo möglich im Sicherheitsprotokoll festhalten. Ein Beispiel wäre der Versuch, auf ein geschütztes Datenobjekt zuzugreifen, für welches keine Berechtigung existiert. 2. Der Hersteller SOLL anhand einer Design-Dokumentation in hinreichender Detailtiefe nachweisen, dass die Anforderungen hinreichend implementiert wurden.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung einer Funktionsprüfung der entsprechenden Mechanismen zur Erkennung von unbefugtem Zugang wird empfohlen. 2. Die Durchführung von Penetrationstests wird empfohlen, um sicherzustellen, dass diese Designanforderung hinreichend implementiert wurde.
SAR_02.ZS	**Anforderung**
	Das Zentrale System MUSS Funktionen zur Verhinderung und Erkennung von unbefugtem Zugang unterstützen.

	Insbesondere MÜSSEN im Zentralen System Schnittstellen zur Intrusion Detection und Monitoring Systeme bereitgestellt werden.
	Empfehlung und Umsetzungserläuterungen
	1. Es SOLLEN Mechanismen implementiert werden, die den Versuch von unbefugtem Zugang erkennen und wo möglich im Sicherheitsprotokoll festhalten. Ein Beispiel wäre der Versuch, auf ein geschütztes Objekt zuzugreifen, für welches keine Berechtigung existiert. 2. Der Hersteller SOLL anhand einer Design-Dokumentation in hinreichender Detailtiefe nachweisen, dass die Anforderungen hinreichend implementiert wurden.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung einer Funktionsprüfung der entsprechenden Mechanismen zur Erkennung von unbefugtem Zugang wird empfohlen. 2. Die Durchführung von Penetrationstests wird empfohlen, um sicherzustellen, dass diese Designanforderung hinreichend implementiert wurde.
SAR_03.ZL	**Anforderung**
	Sowohl erfolgreiche Logins als auch fehlgeschlagene Loginversuche MÜSSEN im Sicherheitsprotokoll des Zählers erfasst werden.
	Empfehlung und Umsetzungserläuterungen
	1. Bei der Implementierung des Sicherheitsprotokolls ist zu beachten, dass die Einträge nicht andere sicherheitsrelevante Protokolleinträge überschreiben.

	2. Nach einer definierbaren Anzahl von fehlerhaften Loginversuchen SOLL der Zähler das Zentrale System benachrichtigen. 3. Der Hersteller SOLL anhand einer Design-Dokumentation in hinreichender Detailtiefe nachweisen, dass die Anforderungen hinreichend implementiert wurden.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung einer Funktionsprüfung des Erstellens von Einträgen im Sicherheitsprotokoll wird empfohlen. 2. Die Durchführung von Penetrationstests wird empfohlen, um sicherzustellen, dass diese Designanforderung hinreichend implementiert wurde.
SAR_03.GW	**Anforderung**
	Sowohl erfolgreiche Logins als auch fehlgeschlagene Loginversuche MÜSSEN im Sicherheitsprotokoll des Gateways erfasst werden.
	Empfehlung und Umsetzungserläuterungen
	1. Bei der Implementierung des Sicherheitsprotokolls ist zu beachten, dass die Einträge nicht andere sicherheitsrelevante Protokolleinträge überschreiben. 2. Nach einer definierbaren Anzahl von fehlerhaften Loginversuchen SOLL das Gateway das Zentrale System benachrichtigen. 3. Der Hersteller SOLL anhand einer Design-Dokumentation in hinreichender Detailtiefe nachweisen, dass die Anforderungen hinreichend implementiert wurden.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung einer Funktionsprüfung des Erstellens von

	Einträgen im Sicherheitsprotokoll wird empfohlen. 2. Die Durchführung von Penetrationstests wird empfohlen, um sicherzustellen, dass diese Designanforderung hinreichend implementiert wurde.
SAR_03.ZS	**Anforderung**
	Sowohl erfolgreiche Logins als auch fehlgeschlagene Loginversuche MÜSSEN in den Sicherheitsprotokollen des Zentralen Systems erfasst werden.
	Empfehlung und Umsetzungserläuterungen
	1. Bei der Implementierung des Sicherheitsprotokolls ist zu beachten, dass die Einträge nicht andere sicherheitsrelevante Protokolleinträge überschreiben. 2. Der Hersteller SOLL anhand einer Design-Dokumentation in hinreichender Detailtiefe nachweisen, dass die Anforderungen hinreichend implementiert wurden.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung einer Funktionsprüfung des Erstellens von Einträgen im Sicherheitsprotokoll wird empfohlen. 2. Die Durchführung von Penetrationstests wird empfohlen, um sicherzustellen, dass diese Designanforderung hinreichend implementiert wurde.

C.5 Vertraulichkeit

Anf._ID	
SCR_01.ZL	**Anforderung**
	Folgende Schnittstellen am Zähler MÜSSEN Verschlüsselung auf der Anwendungsschicht mit einem zugelassenen Algorithmus unterstützen: • LAN zwischen Stromzähler und Zentralem System, • WAN zwischen Stromzähler und Zentralem System, • Multi-Utility-Schnittstelle zwischen Stromzähler und Spartenzähler, • Kundenschnittstelle.
	Empfehlung und Umsetzungserläuterungen
	1. Die zulässigen kryptografischen Algorithmen sind in Anforderung SPR_01 zu finden. 2. Die Kommunikation SOLL mittels symmetrischer Kryptografie gesichert werden, bei der die Daten sowohl verschlüsselt als auch authentifiziert werden. Hierbei ist Anforderung SPR_01 zu beachten.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung einer Funktionsprüfung wird empfohlen. Hierbei soll konkret überprüft werden, dass die genannten Schnittstellen die zulässigen kryptografischen Algorithmen tatsächlich unterstützen.
SCR_01.GW	**Anforderung**
	Für Wartungszwecke des Gateways über das Zentrale System MUSS die WAN-Schnittstelle am Gateway Verschlüsselung auf der Anwendungsschicht mit einem zugelassenen kryptografischen Verfahren unterstützen.

	Empfehlung und Umsetzungserläuterungen
	1. Die zulässigen kryptografischen Algorithmen sind in Anforderung SPR_01 zu finden. 2. Die Kommunikation SOLL mittels symmetrischer Kryptografie gesichert werden, bei der die Daten sowohl verschlüsselt als auch authentifiziert werden. Hierbei ist Anforderung SPR_01 zu beachten.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung einer Funktionsprüfung wird empfohlen. Hierbei soll konkret überprüft werden, dass die genannten Schnittstellen die zulässigen kryptografischen Algorithmen tatsächlich unterstützen.
SCR_01.ZS	**Anforderung**

	Folgende Schnittstellen im Zentralen System MÜSSEN Verschlüsselung auf der Anwendungsschicht mit einem zugelassenen Algorithmus unterstützen:
	• WAN_Z zwischen Stromzähler und Zentralem System;
	• WAN_GW:
	  ○ zwischen Stromzähler und Zentralem System,
	  ○ zwischen Gateway und Zentralem System, falls die Schnittstelle zu Wartungszwecken genutzt wird;
	• Benutzerschnittstellen (UI);
	• Alle internen Schnittstellen des Zentralen System (Zone zu Zone);
	• Internetschnittstelle des Kundenportals;
	• Schnittstelle am MDMS zum Back-End System.

	Empfehlung und Umsetzungserläuterungen
	1. Die zulässigen kryptografischen Algorithmen sind in Anforderung SPR_01 zu finden. 2. Zonen im Zentralen System sind in Anforderung SRR_04.ZS näher beschrieben.

	3. Schnittstellen innerhalb des Zentralen Systems sind in Kapitel B.2 näher beschrieben.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung einer Funktionsprüfung wird empfohlen. Hierbei soll konkret überprüft werden, dass die genannten Schnittstellen die zulässigen kryptografischen Algorithmen tatsächlich unterstützen.

C.6 Auditierung und Protokolle

Anf._ID	
SLR_01.ZL	**Anforderung**
	Der Zähler MUSS eine lokale Auditierung für alle Sicherheitsereignisse unterstützen. Zusätzlich zu den existierenden Protokollen (Logdatei/Logbuch), MUSS hierfür ein dediziertes Sicherheitsprotokoll existieren, in welchem die Sicherheitsereignisse gespeichert werden. Der Zähler MUSS weiterhin dedizierte Register besitzen, um die Häufigkeit der aufgetretenen Sicherheitsereignisse innerhalb eines bestimmten Zeitraums zu protokollieren. Dieser Zeitraum MUSS konfigurierbar sein. Der Zähler MUSS mindestens die in Kapitel B.4 beschriebenen Sicherheitsereignisse protokollieren.
	Empfehlung und Umsetzungserläuterungen
	1. Im Sicherheitsprotokoll SOLL soweit möglich zu jedem Eintrag jeweils

	die Kennung (ID) des verursachenden Benutzers bzw. Systems, die Schnittstelle, der Ereignis-Typ, der Zeitpunkt, sowie das Ergebnis der Aktion gespeichert werden. 2. Der Hersteller SOLL ein Verzeichnis aller unterstützten Sicherheitsereignisse angeben.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Verifizierung der Anforderung anhand einer Funktionsprüfung des Sicherheitsprotokolls. 2. Die Durchführung von Penetrationstests wird empfohlen, um sicherzustellen, dass diese Designanforderung hinreichend implementiert wurde.
SLR_01.GW	**Anforderung**
	Das Gateway MUSS eine lokale Auditierung für alle Sicherheitsereignisse unterstützen. Zusätzlich zu den existierenden Protokollen (Logdatei/Logbuch), MUSS hierfür ein dediziertes Sicherheitsprotokoll existieren, in welchem die Sicherheitsereignisse gespeichert werden. Das Gateway MUSS mindestens die in Kapitel B.4 beschriebenen Sicherheitsereignisse protokollieren.
	Empfehlung und Umsetzungserläuterungen
	1. Im Sicherheitsprotokoll SOLL soweit möglich zu jedem Eintrag jeweils die Kennung (ID) des verursachenden Benutzers bzw. Systems, die Schnittstelle, der Ereignis-Typ, der Zeitpunkt, sowie das Ergebnis der Aktion gespeichert werden. 2. Der Hersteller SOLL ein Verzeichnis aller unterstützten

	Sicherheitsereignisse angeben.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Verifizierung der Anforderung anhand einer Funktionsprüfung des Sicherheitsprotokolls. 2. Die Durchführung von Penetrationstests wird empfohlen, um sicherzustellen, dass diese Designanforderung hinreichend implementiert wurde.
SLR_01.ZS	**Anforderung**
	Das Zentrale System MUSS eine lokale Auditierung für alle Sicherheitsereignisse unterstützen. Zusätzlich zu den existierenden Protokollen (Logdatei/Logbuch), MUSS hierfür ein dediziertes Sicherheitsprotokoll existieren, in welchem die Sicherheitsereignisse gespeichert werden oder es MUSS die Möglichkeit geben in einem Protokoll dediziert nach allen Sicherheitsereignissen zu filtern.
	Empfehlung und Umsetzungserläuterungen
	1. Im Sicherheitsprotokoll SOLL soweit möglich zu jedem Eintrag jeweils die Kennung (ID) des verursachenden Benutzers bzw. Systems, die Schnittstelle, der Ereignis-Typ, der Zeitpunkt, sowie das Ergebnis der Aktion gespeichert werden. 2. Der Hersteller SOLL ein Verzeichnis aller unterstützten Sicherheitsereignisse angeben.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Verifizierung der Anforderung anhand einer Funktionsprüfung des

	Sicherheitsprotokolls. 2. Die Durchführung von Penetrationstests wird empfohlen, um sicherzustellen, dass diese Designanforderung hinreichend implementiert wurde.
SLR_02	**Anforderung**
	Die Einträge aller Protokolle MÜSSEN vor unbefugten Veränderungen geschützt sein.
	Empfehlung und Umsetzungserläuterungen
	1. Das Sicherheitsprotokoll SOLL mittels rollenbasierter Zugangskontrolle geschützt sein.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Die Durchführung von Penetrationstests wird empfohlen, um sicherzustellen, dass diese Designanforderung hinreichend implementiert wurde.
SLR_03.ZL	**Anforderung**
	Der Speicher für das Sicherheitsprotokoll des Zählers MUSS mindestens die letzten 100 Sicherheitsereignisse speichern. Das Sicherheitsprotokoll MUSS als rollierendes Protokoll umgesetzt werden.
	Empfehlung und Umsetzungserläuterungen
	1. Der Hersteller SOLL anhand einer Design-Dokumentation in

	hinreichender Detailtiefe nachweisen, dass die Anforderungen hinreichend implementiert wurden.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Verifizierung der Anforderung anhand einer Funktionsprüfung, um sicherzustellen, dass das Sicherheitsprotokoll hinreichende Kapazitäten aufweist.
SLR_03.GW	**Anforderung**
	Der Speicher für das Sicherheitsprotokoll des Gateways MUSS mindestens die letzten 1000 Sicherheitsereignisse speichern. Das Sicherheitsprotokoll MUSS als rollierendes Protokoll umgesetzt werden.
	Empfehlung und Umsetzungserläuterungen
	1. Der Hersteller SOLL anhand einer Design-Dokumentation in hinreichender Detailtiefe nachweisen, dass die Anforderungen hinreichend implementiert wurden.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Verifizierung der Anforderung anhand einer Funktionsprüfung, um sicherzustellen, dass das Sicherheitsprotokoll hinreichende Kapazitäten aufweist.
SLR_03.ZS	**Anforderung**
	Die Komponenten des Zentralen Systems MÜSSEN eine Anbindung an einen Protokollserver unterstützen.

	Es MUSS möglich sein, den Protokollserver auf einem dedizierten System (d.h. nicht auf dem HES, MDMS oder KMS) zu betreiben.
	Empfehlung und Umsetzungserläuterungen
	1. Für das Zentrale System SOLL ein dedizierter Protokollserver (z.B. Syslog-Server) vorhanden sein. Dieser Protokollserver SOLL die Sicherheitsereignisse von allen Komponenten des Zentralen Systems protokollieren. 2. Der Hersteller SOLL anhand einer Design-Dokumentation in hinreichender Detailtiefe nachweisen, dass die Anforderungen hinreichend implementiert wurden.
	Empfohlene Qualitätssicherungsmaßnahmen
	1. Verifizierung der Anforderung anhand einer Funktionsprüfung, um sicherzustellen, dass der Protokollserver die Sicherheitsereignisse sachgemäß verwaltet.

C.7 Produktlebenszyklus-Management

Anf._ID	
SDR_01	**Anforderung**
	Der Hersteller MUSS spätestens bei Lieferung eine Zertifizierung nach ISO/IEC 27001 für alle sicherheitsrelevanten Entwicklungs-, Fertigungs- und Provisionierungsprozesse für Geräte und Produkte vorweisen, welche im Smart Metering System (Zähler, Gateways und Zentrale Systeme) eingesetzt werden.
	Empfehlung und Umsetzungserläuterungen
	1. Die Anforderung gilt für alle sicherheitsrelevanten Entwicklungs-, Fertigungs- und Provisionierungsprozesse für Zähler und Gateway. 2. Weiterhin gilt die Anforderung für die Entwicklungs- und Provisionierungsprozesse des Zentralen Systems. 3. Sollten sicherheitsrelevante Komponenten von Zulieferern bezogen werden, so SOLLEN diese Bereiche und entsprechende Übergabeprozesse des Zulieferers eine Zertifizierung nach ISO/IEC 27001 vorweisen. 4. Zusätzlich SOLL ISO/IEC 27001 für sicherheitsrelevante Tools und Geräte Anwendung finden, welche mit der Smart Metering Architektur genutzt werden. Beispielsweise Handheld Terminals oder Wartungssoftware. 5. Der Hersteller SOLL die Sicherheitsrichtlinien des Unternehmens offenlegen.
SDR_02	**Anforderung**
	Der Hersteller MUSS ein gesichertes Konfigurationsmanagementsystem für die Verwaltung der Produkte einsetzen. Alle Änderungen der darin hinterlegten Informationen MÜSSEN zweckmäßig, nachvollziehbar und dokumentiert sein.

	1. Adäquate IT- und physikalische Sicherheitsmaßnahmen MÜSSEN beim Hersteller implementiert sein, um das Konfigurationsmanagementsystem zu schützen. 2. Der Hersteller MUSS einen Auditmechanismus bereitstellen, welcher den Autor jeder Änderung identifizieren kann. 3. Zulieferer MÜSSEN vergleichbare Prozesse implementieren, sofern diese sicherheitsrelevante Funktionen bereitstellen.
	Empfehlung und Umsetzungserläuterungen
	1. Die Anforderung bezieht sich sowohl auf die Prozesse zur Entwicklung und Fertigung des Zählers, des Gateways als auch des Zentralen Systems. 2. Folgende Beispiele für den Funktionsumfang eines gesichertes Konfigurationsmanagementsystem SOLLEN berücksichtig werden: • Verwaltung der Hardwarekonfigurationen und dessen Änderungen für die Geräte. • Verwaltung von Quelltexten (Sourcecode) und dessen Änderungen der Firmware oder Software. • Verwaltung von (kundenspezifischen) Konfigurationsparametern und dessen Änderungen für die Geräte.
SDR_03	**Anforderung**
	Gesicherter Versionierungsprozess: 1. Alle freigegebenen Versionen (Hardware sowie Firmware) eines Gerätes oder Produktes MÜSSEN vom Hersteller eindeutig identifiziert werden. 2. Firmware MUSS anhand eines sicheren Hashwertes identifizierbar sein. 3. Es MUSS dem Hersteller möglich sein, freigegebene Versionen von Geräten innerhalb ihres Produktlebenszyklus‘ unter Nachweis der Hashwerte zu reproduzieren. 4. Austauschbare Hardwareteile (Module) MÜSSEN eine gesonderte Versionierung aufweisen.

	5. Software oder Software-Updates MÜSSEN anhand ihrer Hashwerte identifizierbar sein.
	Empfehlung und Umsetzungserläuterungen
	1. Die Anforderung bezieht sich auf die Versionierungsprozesse zur Entwicklung der Firmware des Zählers und des Gateways. 2. Weiterhin bezieht sich die Anforderung auf die Versionierungsprozesse zur Entwicklung von Software, die im Zentralen System eingesetzt wird. 3. Die zulässigen kryptografischen Hashfunktionen sind in Anforderung SPR_01 zu finden. 4. Ein Beispielprozess für das Erstellen von digitalen Signaturen ist unter A.2 beschrieben.
SDR_04	**Anforderung**
	Der Hersteller MUSS einen Fehlersanierungs- und Meldeprozess implementieren: 1. Der Hersteller MUSS sich aktiv an der Überwachung und Prüfung von Schwachstellen beteiligen, über Sicherheitslücken umgehend informieren und Updates, welche Schwachstellen beheben, unter Einbeziehung aller technischen Möglichkeiten zeitnah bereitstellen. 2. Hersteller MÜSSEN über Prozesse verfügen, um extern berichtete Sicherheitslücken zu behandeln.
	Empfehlung und Umsetzungserläuterungen
	1. Die Anforderung bezieht sich auf die Fehlersanierungs- und Meldeprozesse bei der Entwicklung und Fertigung des Zählers, des Gateways und des Zentralen Systems. 2. Folgende Beispiele für einen Fehlersanierungs- und Reportingprozess SOLLEN berücksichtig werden: • Identifikation und Behandlung von vom Hersteller gefundenen

	Fehlern. • Identifikation und Behandlung von vom Geräte- oder Systembetreiber berichteten Fehlern. • Identifikation und Behandlung von von Externen berichteten Fehlern; beispielsweise Sicherheitslücken, die von Forschern entdeckt wurden.
SDR_05	**Anforderung**
	Der Hersteller MUSS umfangreiche Tests der Produkte durchführen. Diese Tests MÜSSEN auch Sicherheitstests beinhalten. 1. Alle Geräte MÜSSEN den Spezifikationen der vom Hersteller gelieferten Dokumentation entsprechen. 2. Durch Verwendung von nicht-trivialen Testfällen MUSS der Hersteller in der Lage sein, die Sicherheit und funktionale Korrektheit der Produkte zu demonstrieren. 3. Die Tests MÜSSEN den gesamten Funktionsumfang des Produkts abdecken und insbesondere Tests der gesamten Kommunikationskette beinhalten. 4. Sowohl häufig genutzte Funktionen als auch selten verwendete Funktionen wie zum Beispiel Software-Updates MÜSSEN hinreichend getestet werden. 5. Der Hersteller MUSS dem Netzbetreiber bei Freigabe neuer Produktversionen Ergebnisse von durchgeführten Sicherheitstests zur Verfügung stellen.
	Empfehlung und Umsetzungserläuterungen
	1. Die Anforderung bezieht sich auf die Sicherheitstests für den Zählers, das Gateway und das Zentrale System. 2. Folgende Beispiele für die Durchführung von Sicherheitstests SOLLEN berücksichtig werden: • Fuzzing Tests

	• Tests der Designstabilität (Robustheitstests) • Penetrationstests Siehe Anhang B für Erläuterungen zu den genannten Tests.
SDR_06	**Anforderung**
	Der Hersteller MUSS ein hohes IKT Sicherheitsbewusstsein (Security–Awareness) besitzen und Schulungen zur IKT Sicherheit für das Personal anbieten. Der Hersteller MUSS darlegen, dass er das nötige Know-How besitzt, um sichere Produkte zu entwickeln und zu produzieren. Der Hersteller MUSS einen technischen Ansprechpartner für den Bereich Sicherheit benennen.
	Empfehlung und Umsetzungserläuterungen
	1. Beispiel: • Nachweisbare Berufspraxis in den relevanten Bereichen oder Sicherheitszertifizierung wie z.B. nach CISSP oder CISM.
SDR_07	**Anforderung**
	Es MÜSSEN Funktionen zur Erhöhung der Sicherheit der zugrundeliegenden Plattform, Implementierungssprache und Werkzeugkette berücksichtigt werden. Sollte dies nicht erforderlich oder möglich sein, MUSS dies entsprechend nachgewiesen werden.
	Empfehlung und Umsetzungserläuterungen
	1. Beispiele: • Gesicherter Bootprozess, in welchem der Bootloader die Echtheit der auszuführenden Firmware verifiziert. • Deaktivieren von Hardwaredebugschnittstellen wie z.B. JTAG. • Aktivieren von Funktionen zur Read-Out-Protection eines

	Mikrokontrollers.
SDR_08	**Anforderung**
	Sicheres Provisionieren von kryptografischem Schlüsselmaterial MUSS innerhalb des Fertigungsprozesses vom Hersteller durchgeführt werden. Es MUSS möglich sein, jegliches kryptografisches Schlüsselmaterial der Geräte innerhalb des Fertigungsprozesses individuell zu provisionieren. Der Hersteller MUSS einen sicheren Übergabeprozess zum Geräte- oder Systembetreiber etablieren.
	Empfehlung und Umsetzungserläuterungen
	1. Beispiele: • Der Hersteller MUSS einen sicheren Produktionsbereich gewährleisten, um das sichere initiale Provisionieren von Schüsselmaterial durchführen zu können. • Ein sicherer Übergabeprozess aller in das Gerät eingespielten Informationen an das Zentrale System MUSS etabliert werden. • Ein Beispielprozess für das gesicherte Provisionieren ist unter A.1 beschrieben.
SDR_09	**Anforderung**
	Für Komponenten des Zentralen Systems, die eine Fernwartungsfunktion einer dritten Partei bereitstellen, ist ein Sicherheitskonzept vorzulegen und detailliert zu dokumentieren.
	Empfehlung und Umsetzungserläuterungen
	1. Fernwartungsfunktionen SOLLEN wo möglich vermieden werden. 2. Ein Terminalserver stellt ein Beispiel für die Sicherung einer Fernwartungsfunktion dar.

Anhang A Beispielprozesse

Die hier beschriebenen Prozesse sind Beispiele wie ausgewählte Anforderungen im Sinne der Ende-zu-Ende Sicherheit umgesetzt werden können. Die folgenden Kapitel mit Beispielprozessen sind nicht im normativen Sinne sondern als Verständnishilfe zu interpretieren.

Anhang A.1 Prozess zur Einspielung von kryptografischem Schlüsselmaterial (Provisionierung)

Eine der wichtigsten Anforderungen an die Sicherheitsarchitektur des Smart Metering Systems ist die Verwendung von kryptografischem Schlüsselmaterial, welches pro Gerät und auch pro modellierter Rolle auf einem Gerät verschieden sein muss. Das kryptografische Schlüsselmaterial muss zufällig erzeugt werden und initial sicher in das Gerät eingebracht werden.

Zur Optimierung der Inbetriebnahmeprozesse und der gleichzeitigen Wahrung der Sicherheit, ist es angedacht, das Einspielen von kryptografischem Schlüsselmaterial beim Hersteller als einen der letzten Schritte in der Produktionskette durchzuführen. Dieses initiale kryptografische Schlüsselmaterial wird genutzt, um eine erste, sichere Verbindung mit den Geräten herzustellen, beispielsweise vom Zentralen System oder dem Handheld Terminal. Die Sicherheit der Kommunikation zwischen diesen Geräten basiert somit auf den vom Hersteller etablierten Prozessen zum Einbringen des kryptografischen Schlüsselmaterials.

Hierbei ergeben sich die folgenden Hauptpunkte, welche zu berücksichtigen sind:

- Anforderungen an die Vertrauenswürdigkeit der Prozessumgebung
- Anforderungen an die Prozesse zum Erzeugen und Einspielen des kryptografischen Schlüsselmaterials
- Anforderungen an die Übergabeprozesse des eingebrachten kryptografischen Schlüsselmaterials

Es ist dringend empfohlen die beschriebenen Bereiche nach ISO27001 zu zertifizieren.

Anhang A.1.1 Anforderungen an die Prozessumgebung

Die Prozessumgebung selbst muss verschiedene Anforderungen erfüllen, um die Vertrauenswürdigkeit des eingespielten kryptografischen Schlüsselmaterials herstellen zu können.

Hierbei muss zuerst die Vertrauenswürdigkeit der Hardware vom Hersteller garantiert werden können, auf welcher das kryptografische Schlüsselmaterial eingespielt werden soll. Der Hersteller muss nachweisen, dass keine Manipulation der Hardware erfolgt ist.

Weiterhin muss sichergestellt werden, dass die Vertrauenswürdigkeit der Firmware auf dem Gerät gegeben ist. Der Hersteller muss den Nachweis erbringen können, dass die Authentizität der Firmware des zu provisionierenden Gerätes gegeben ist.

Als dritter Punkt muss die Sicherheit des Provisionierungsbereiches selbst gegeben sein. Dies umfasst insbesondere die Sicherheit der verwendeten IT Komponenten und die physikalischen Zugangskontrollen des Provisionierungsbereiches.

Anhang A.1.2 Anforderungen an das Erzeugen und Einspielen

Das Erzeugen, Einspielen und Speichern von kryptografischem Schlüsselmaterial soll in einer gesicherten Prozessumgebung erfolgen.

Zum Erzeugen des kryptografischen Schlüsselmaterials soll ein zugelassener Zufallszahlengenerator verwendet werden, wie in Anforderung SPR_02 beschrieben.

Es ist im Folgenden zu unterscheiden, ob ein symmetrischer Schlüssel oder privates/öffentliches Schlüsselpaar genutzt werden soll:

- Initiale Symmetrische Schlüssel sollen außerhalb des Gerätes, innerhalb der gesicherten Prozessumgebung unter Verwendung eines externen Zufallszahlengenerators erzeugt werden. Der so erzeugte Schlüssel wird in das Gerät eingespielt.

- Das privates/öffentliche Schlüsselpaar soll innerhalb des Gerätes und innerhalb der gesicherten Prozessumgebung generiert werden. Teile der Entropie für die Erzeugung des privaten Schlüssels sollen durch einen externen Zufallszahlengenerator erzeugt werden. Entsprechende Zufallsdaten sollen in das Gerät eingespielt werden. Nach Generierung des Schlüsselpaares darf nur der öffentliche Schlüssel in Form eines Certificate Signing Requests (CSRs) vom Gerät ausgelesen werden können. Nach der Verarbeitung des CSRs in ein valides Gerätezertifikat, muss dieses zusammen mit weiteren Informationen (z.B. Root Zertifikate) sicher in das Gerät eingespielt werden.

Jegliches Schlüsselmaterial welches auf den Geräten genutzt wird, soll schon innerhalb des Provisionierungsprozesses beim Hersteller individuell initialisiert werden.

Anhang A.1.3 Anforderungen an die Übergabe

Der Hersteller und der Betreiber des zentralen Systems müssen gemeinsam ein gesichertes Austauschverfahren für das provisionierte kryptografische Schlüsselmaterial etablieren. Hierbei muss sichergestellt werden, dass die Vertraulichkeit und Authentizität des eingebrachten kryptografischen Schlüsselmaterials bei der Übergabe gewährleistet bleibt.

Ein solcher Übergabeprozess kann beispielsweise durch die Verwendung von Verschlüsselungsverfahren und digitalen Signaturen modelliert werden:

> Hersteller und Betreiber des Zentralen Systems können je ein privates/öffentliches Schlüsselpaar erzeugen und ihre öffentlichen Schlüssel auf sicheren Wege, d.h. unter Verwendung einer Zertifikatsstruktur (PKI), austauschen.
>
> Die Echtheit der ausgetauschten öffentlichen Schlüssel muss unbedingt überprüft und dokumentiert werden.

Der Hersteller verwendet nun den erhaltenen öffentlichen Schlüssel zur Verschlüsselung aller auf den Geräten eingebrachten schützenswerten Daten (z.B. alle individuell erzeugten Schlüssel pro Rolle auf einem Gerät).

Diese verschlüsselten Daten werden vom Hersteller in einen elektronischen Lieferschein oder vergleichbares Dokument aufgenommen, welcher bzw. welches durch den Betreiber des Zentralen Systems verarbeitet werden kann. Hierbei erfolgt eine Zuordnung von Seriennummer (oder anderweitige eindeutige Gerätekennung) eines Gerätes zu verschlüsselter Information. Bevor dieser Lieferschein an den Betreiber des zentralen Systems verschickt wird, signiert der Hersteller diesen unter Verwendung seines eigenen privaten Schlüssels.

Der Betreiber des Zentralen Systems überprüft bei Empfang des elektronischen Lieferscheins die digitale Signatur des Herstellers durch Verwendung seines öffentlichen Schlüssels und verifiziert somit die Echtheit des empfangenden Dokumentes.

Als zweiten Schritt kann der Betreiber des Zentralen Systems die vom Hersteller verschlüsselten Informationen entschlüsseln und das Material in das Zentrale System importieren.

Hierbei ergeben sich vergleichbare Anforderungen an die Sicherung des Zugriffs auf die jeweiligen privaten Schlüssel wie unter „Firmware-Update-Prozess“ beschrieben.

Anhang A.2 Firmware-Update-Prozess

Die Integrität einer Firmware-Datei wird durch das Anhängen einer digitalen Signatur sichergestellt. Das Gerät, für welches die Firmware bestimmt ist, kann anhand der digitalen Signatur verifizieren, dass die Firmware-Datei tatsächlich vom Hersteller stammt. Das Gerät darf die Firmware-Datei nur akzeptieren, wenn es anhand der digitalen Signatur die Urheberschaft des Herstellers eindeutig verifizieren kann.

Um einer solchen digitalen Signatur eine entsprechende Bedeutung zusprechen zu können, muss der Hersteller einen Prozess für das sichere Erzeugen von digitalen Signaturen festlegen.

Anhang A.2.1 Hintergrund digitales Signieren

Bei der Erstellung einer digitalen Signatur wird zunächst der Hashwert der Firmware-Datei berechnet. Die digitale Signatur ist die Ausgabe der Verschlüsslung des Hashwertes mithilfe des privaten Schlüssels des Herstellers. Bei Empfang der Firmware-Datei verifiziert das Gerät die digitale Signatur mit dem öffentlichen Schlüssel durch Vergleichen mit dem Hashwert der empfangenen Datei.

Hierbei ergeben sich die folgenden Hauptpunkte, welche zu berücksichtigen sind:

- Anforderungen an den Freigabeprozess für Firmware-Updates.

- Anforderungen an den Prozess zum Zugriff und der Sicherung des geheimen kryptografischen Schlüsselmaterials, mit welchem die digitale Signatur der Firmware-Datei erstellt wird (vergleiche Anforderungen zur Schlüsselverwaltung).
- Anforderungen an den Prozess zur gesicherten Einspielung des öffentlichen kryptografischen Schlüsselmaterials in die Geräte (vergleiche Anforderung SDR_07).
- Anforderungen an den Aktualisierungsprozess des Gerätes selbst (vergleiche Anforderungen SIR_03.*).

Es ist dringend empfohlen die beschriebenen Bereiche nach ISO27001 zu zertifizieren (vergleiche Anforderung SDR_01).

Dieses Kapitel beschreibt geeignete Beispielprozesse und entsprechende Anforderungen unter dem Aspekt der IKT Sicherheit.

Anhang A.2.2 Freigabeprozess

Der Hersteller sollte einen Freigabeprozess für neue Firmware-Versionen etablieren. Der Hersteller sollte eine für den Freigabeprozess verantwortliche Person bestimmen.

Der Freigabeprozess ist vom Hersteller zu dokumentieren. Der Prozess muss entsprechende Nachweise über die Freigabe der Firmware-Versionen liefern. Es muss festgehalten werden, welche Person zu welchem Zeitpunkt die Freigabe des Firmware-Updates autorisiert hat.

Die Version des Firmware-Updates ist anhand ihres Hashwertes zu dokumentieren. Sollte ein Firmware-Update aus mehreren Komponenten (verschiedene Dateien) bestehen, so sind diese einzeln zu benennen und anhand ihres Hashwertes zu dokumentieren. Durch die Autorisierung der Freigabe eines Firmware-Updates wird vom Hersteller belegt, dass die Firmware-Datei eindeutig mit ihrem Hashwert identifiziert werden kann.

Anhang A.2.3 Verwaltung und Sicherung des geheimen Schlüsselmaterials

Nach Freigabe einer Firmware muss für diese eine digitale Signatur erstellt werden. Sollte ein Firmware-Update aus mehreren Komponenten (verschiedene Dateien) bestehen, so sind diese einzeln zu signieren.

Der Hersteller muss hierfür ein System zu betreiben, welches den Zugriff auf das geheime Schlüsselmaterial regelt, welches zur Signaturerzeugung von Firmware-Updates eingesetzt werden soll.

Dieses System ist in einer gesicherten IT-Umgebung zu betreiben.

Der Hersteller sollte eine verantwortliche Person für die Erzeugung der digitalen Signatur bestimmen. Diese Person muss dann für die Firmware eine digitale Signatur durch das System erstellen lassen.

Hierbei darf es nicht möglich sein, dass diese Personen direkten Zugriff auf die entsprechenden Schlüssel erhalten. Das System darf nur Funktionen bereitstellen, die die Firmware digital signieren. Weiterhin muss das System einen Auditierungsmechanismus

bereitstellen, welcher für die Ausstellung von digitalen Signaturen Nachweise über Zeitpunkt, Person, Firmware-Version und Hashwert der Firmware erbringen kann.

Das System soll weiterhin das geheime Schlüsselmaterial hinreichend vor physikalischem Zugriff schützen, beispielsweise durch Ablage auf einem gesicherten Hardware Modul.

Nach erfolgreichem Erzeugen der Signatur kann die freigegebene Firmware-Version zusammen mit der Signatur zum finalen Firmware-Update kombiniert werden. Dieses Firmware-Update wird dann dem Betreiber des zentralen Systems zur Verfügung gestellt.

Anhang A.2.4 Einspielungssprozess

Um die maschinelle Verifikation der digitalen Signatur eines Firmware-Updates zu ermöglichen, muss auf einem Gerät das korrespondierende öffentlich Schlüsselmaterial eingespielt (provisioniert) sein.

Dieser Einspielprozess des öffentlichen Schlüsselmaterials muss initial beim Hersteller in einer gesicherten Umgebung erfolgen. Dieser Einspielprozess garantiert somit die Authentizität des öffentlichen Schlüsselmaterials, welches auf das Gerät eingebracht wird.

Das öffentliche Schlüsselmaterial darf im Anschluss nur durch ein autorisiertes (digital signiertes) Firmware-Update veränderbar sein.

Dieser Einspielprozess erfolgt im Idealfall zusammen mit dem Einspielen mit allem benötigten kryptografischen Schlüsseln.

Anhang A.2.5 Updateprozess des Gerätes

Bevor ein Gerät eine Firmware-Datei zum Update akzeptieren darf, muss es dessen digitale Signatur überprüfen. Das Einspielen darf nicht erfolgen, sollte die Verifikation fehlschlagen oder eine digitale Signatur gänzlich fehlen. Das Gerät kann somit sicherstellen, dass die empfangene Firmware-Datei authentisch ist, das heißt tatsächlich vom Hersteller stammt.

Anhang A.3 Firmware-Aktualisierungsprozess

Ein Multicast ist eine sinnvolle Methode, um Firmware-Updates, die signifikante Bandbreite benötigen, an mehrere Endgeräte zugleich zu versenden. Gemäß der IMA-VO müssen die entsprechenden Daten auch im Multicast verschlüsselt und authentifiziert werden. Daher wird der Multicast durch individuelle Unicasts eingeleitet.

Hieraus ergibt sich folgender Beispielprozess:

1. Das Zentrale System erzeugt einen temporären Multicast-Schlüssel. Dieser Multicast-Schlüssel ist zwar identisch für alle Endgeräte, muss jedoch mit dem individuellen Schlüssel des Endgeräts verschlüsselt, authentifiziert und an das entsprechende Gerät per Unicast versendet werden.
2. Das Zentrale System versendet das Firmware-Update per Multicast an alle initialisierten Endgeräte. Das Firmware-Update ist mit dem vorher erzeugten Multicast-Schlüssel verschlüsselt und authentifiziert. Anschließend verwirft das Zentrale System den Multicast-Schlüssel.

3. Das Zentrale System versendet eine Aktivierungsnachricht per Unicast an alle initialisierten Endgeräte. Jede Aktivierungsnachricht ist mit dem individuellen Schlüssel des Endgeräts verschlüsselt und authentifiziert.

4. Das Endgerät entschlüsselt und verifiziert die Integrität der Nachricht, die das Firmware-Update enthält. Anschließend verwirft das Endgerät den Multicast-Schlüssel.

5. Des Weiteren überprüft das Endgerät die Integrität der Firmware-Datei anhand der digitalen Signatur und der Gültigkeit der Versionsnummer (siehe auch Anhang A.2).

6. Das Endgerät aktiviert die Firmware, wenn es die Aktivierungsnachricht enthalten, entschlüsselt und deren Integrität verifiziert hat.

Anhang A.4 Gesicherter Eich- oder Prüfprozess

Die folgende Prozessbeschreibung stellt ein Beispiel für die Wahrung der Zählersicherheit beim Durchlaufen eines Eich- oder Prüfprozesses dar. Dieser Beispielprozess kann sowohl für die unternehmensinterne Eichung oder Prüfung als auch die Eichung oder Prüfung durch eine Drittpartei genutzt werden.

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

Der Zähler und das zugehörige Schlüsselmaterial der Rolle „Eich- und Prüfstelle“ muss für die Eich- oder Prüfstelle verfügbar gemacht werden.

Im Key-Management-System wird das Schlüsselmaterial für die Rolle „Eich- oder Prüfstelle“ als *aktiv* markiert. *Aktiv* bedeutet, dass das Schlüsselmaterial für diese Rolle herausgegeben wurde und dass eine Aktualisierung des herausgegebenen Schlüsselmaterials durchgeführt werden muss, sobald dieser Zähler wieder in Betrieb genommen wird.

Die Übergabe des Schlüsselmaterials an eine Eich- oder Prüfstelle kann beispielsweise über eine direkte Anbindung an das Key-Management-System realisiert werden. Alternativ kann das auf dem Zähler provisionierte Schlüsselmaterial exportiert werden und über einen sicheren „Offlineprozess“ übergeben werden. Dies kann beispielsweise ähnlich zum beschriebenen Übergabeprozess in „Einspielung von kryptografischem Schlüsselmaterial beim Hersteller“ erfolgen.

Anhang A.4.2 Herbeiführen des gesicherter Eich- und Prüfmodus

Eine Authentifizierung zwischen Eich- oder Prüfstelle und Zähler muss durchgeführt werden. Hierfür wird das erhaltene Schlüsselmaterial genutzt. Nach erfolgreicher Authentifizierung kann die Eich- oder Prüfstelle den Zähler mit entsprechenden Kommandos den Zähler in den Eichmodus bzw. Prüfmodus versetzen. Jegliche Kommunikation zwischen Zähler und Eich- oder Prüfstelle hat authentifiziert zu erfolgen. Es wird das übergebene Schlüsselmaterial genutzt.

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

Nach erfolgreicher Eichung oder Prüfung muss der Zähler mit einem entsprechenden Kommando in den „*Normalbetrieb*“ zurückgesetzt werden. Die Eich- oder Prüfstelle muss diesen letzten Schritt ausführen, da der gesicherte Eichmodus außerhalb der Eichstelle nicht verfügbar sein darf.

Der Zähler muss die Rolle „Eich- oder Prüfstelle“ bei Übergang zurück den Normalbetrieb zwingend automatisch deaktivieren.

Anhang A.4.3 Übergabe an den Operativen Betrieb

Der Zähler wird von der Eich- oder Prüfstelle zurückgeführt und kann wieder operativ eingesetzt werden. Bei Rückerhalt wird im Key-Management-System das Schlüsselmaterial für die Rolle „Eich- oder Prüfstelle“ als „zu aktualisieren“ gekennzeichnet.

Sobald der Zähler im Feld verbaut und vom Zentralen System erreichbar ist, wird das Schlüsselmaterial für dir Rolle „Eich- oder Prüfstelle“ durch die Rolle „Zentrales System Read-Write“ aktualisiert. Weiterhin wird die Rolle „Eich- oder Prüfstelle“ wird vom Zentralen System wieder aktiviert.

Bei Zählern, die bei der Inbetriebnahme keine Onlineverbindung besitzen, kann vor Ort durch das Handheld Terminal über die Rolle „Maintenance“ die Rolle „Eich- oder Prüfstelle“ mit neuem Schlüsselmaterial versorgt und wieder aktiviert werden.

Anhang B Abkürzungen und Begriffsbestimmungen

Das Verzeichnis dient der Erläuterung im Dokument verwendeter Fachbegriffe und Abkürzungen. Zu detaillierten Beschreibungen von Testprozeduren sowie Hintergründen oder Details der kryptografischen Verfahren wird auf die empfohlene Literatur verwiesen.

Anwendungsschicht	Applikationslayer, **OSI**-Layer 5-7.
Authentifizierung	Authentifizierung wird unterschieden in **Authentifizierung der Kommunikationsteilnehmer** (Beispiel: Mensch, Gerät) und **Authentifizierung von Nachrichten**. Authentifizierung dient der Überprüfung der **Integrität** der Kommunikationsteilnehmer bzw. der Überprüfung der **Datenintegrität**.
Authentifizierung der Kommunikations-teilnehmer	Verifizierung der Identität und **Integrität** der Kommunikationsteilnehmer (Beispiel: Benutzer am Zähler). Darüber hinaus Sicherstellung, dass die Teilnehmer während einer Sitzung fortwährend aktiv (alive) sind. Siehe auch **Passwortauthentifizierung** und **Gegenseitige Authentifizierung**.
Authentifizierung	Die **Authentizität**, also die Echtheit, **der Nachricht** selbst muss

von Nachrichten	gewährleistet sein. Dies erfolgt entweder durch das Anhängen von **Nachrichtenauthentifizierungscodes** (AES-CBC-CMAC) oder durch das Verschlüsseln mittels einer **Blockchiffre in einem Betriebsmodus**, der gleichzeitige **Authentifizierung** unterstützt (z.B. AES-CCM, AES-GCM).
Authentizität	Echtheit.
Bidirektional	Zweiseitig. Siehe auch **Bidirektionale Schnittstelle**.
Bidirektionale Schnittstelle	Bei der Datenübertragung fließen Signale in beide Richtungen.
Blockchiffre	Kryptografisches Verschlüsselungsverfahren, in den Nachrichten von fester Länge verschlüsselt werden.
Broadcast	Datenübertragungstechnik, bei der eine Nachricht zeitgleich an alle Teilnehmer im Netzwerk übermittelt wird. Beim **Multicast** wird die Nachricht an ausgewählte Teilnehmer im Netzwerk gesendet. Beim **Unicast** wird die Nachricht an genauen einen Netzwerkteilnehmer gesendet.
BSI	Bundesamt für Sicherheit in der Informationstechnik in Bonn, Deutschland.
DAVID-VO	Datenformat- und VerbrauchsinformationsdarstellungsVO 2012. Dieser Katalog bezieht sich auf die Version DAVID-VO 2012.
Datenintegrität	Siehe **Integrität** und **Authentifizierung von Nachrichten**.
Digitale Signatur	Dient der Sicherstellung der **Integrität** der Quelle. Bei der Erstellung einer digitalen Signatur wird zunächst der **Hashwert** der Datei berechnet. Die digitale Signatur ist die Ausgabe der Verschlüsslung des **Hashwertes** mithilfe des geheimen Schlüssels des Senders. Der Empfänger verifiziert die digitale Signatur mit dem öffentlichen Schlüssel durch Vergleichen mit dem **Hashwert** der empfangenen Datei. In der Praxis werden **digitale Signaturen** mit auf elliptischen Kurven (**EC**) basierenden Verfahren erstellt.
Display	Siehe *Kapitel B.*
EC	Elliptic Curve. Elliptische Kurven. Siehe auch ENISA [6].

Engineering Menü	Eine Funktionalität des Gerätes, welches Einstellungsänderungen und Informationsabfrage für einen Techniker über das lokale Display des Gerätes übe Tastereingaben erlaubt.
ENISA	European Union Agency for Network and Information Security.
EPRI	Electric Power Research Institute.
Fail-Secure	Konstruktionsprinzip, bei dem sicherheitsrelevante Aspekte so konzipiert sind, dass bei Versagen oder Ausfall die Vertraulichkeit und Integrität des Systems gewährleistet sind
Fuzzing Test	Ein Fuzzing Test wird zur Qualitätssicherung der Software für sichere Netzwerkkommunikation durchgeführt. Dies geschieht durch das Erzeugen eines hohen meist zufälligen Datenvolumens, das auch fehlerhafte Datenpakete enthalten kann, die auf strukturierte Weise in den Datenverkehr eingeschleust werden. Eine ausführliche Einführung in das Thema *Fuzzing* ist in [22] zu finden.
Gateway	Siehe *Kapitel B*.
Gegenseitige Authentifizierung	Bei der gegenseitigen Authentifizierung müssen sich beide Seiten authentifizieren und damit ihre Identität nachweisen. Hierbei finden Challenge-Response Protokolle Anwendung. Andere gängige Methoden benutzen **Zertifikate**.
Gerät	Der Wortlaut „Gerät“ kann sich sowohl auf das Gateway als auch den Zähler beziehen. Dies wird in den Umsetzungserläuterungen beschrieben.
GPRS	General Packet Radio Service.
HAN	Home Area Network.
Handheld Terminal	Ein Gerät, welches ein Techniker verwendet um Einstellungsänderungen und Informationsabfragen über die Wartungsschnittstelle eines Zählers oder Gateways durchzuführen.
Hashfunktion	Funktion die eine Nachricht auf ein Bitfolge (**Hashwert**) bestimmter Länge abbildet. Siehe **Kryptografische Hashfunktion**.
Hashwert	Ausgabe einer **(kryptografischen) Hashfunktion**.

Hybridverfahren	Da **Public-Key Kryptografie** sehr aufwendig ist, kommen Verfahren wie RSA nur in sogenannten Hybridverfahren zum Einsatz. Hierbei werden zufällige symmetrische Sitzungsschlüssel erzeugt (beispielsweise ein 128-bit AES Schlüssel). Der Sitzungsschlüssel wird unter dem öffentlichen Schlüssel des Empfängers verschlüsselt und versandt. Die eigentlichen Nachrichten werden dann mithilfe des Sitzungsschlüssels mit der entsprechenden symmetrischen Chiffre ver- und entschlüsselt.
IETF	*Internet Engineering Task Force.*
IKT Sicherheit	Sicherheit in der Informations- und Kommunikationstechnik.
IMA-VO	Intelligente Messgeräte Anforderungs Verordnung. Dieser Katalog bezieht sich auf die 339. Verordnung ausgegeben am 25. Oktober 2011 Teil II.
Integrität	Die Integrität der Nachricht meint Schutz gegenüber Manipulationen. Siehe auch **Authentifizierung**.
Intrusion Detection System	Ein Intrusion Detection System beobachtet das Verhalten von Komponenten entweder auf der Komponente selbst, oder durch Überwachung der Kommunikation. Bekannte Angriffsmuster oder Anomalien können so erkannt und gemeldet werden.
ISO 27001	ISO Standard für Sicherheit in der Informations- und Kommunikationstechnik.
Konfigurations-managementsystem	Das Konfigurationsmanagementsystem stellt das System beim Hersteller dar, welches den Produktlebenszyklus des Gerätes von seiner Entwicklung über Herstellung und Lieferung verwaltet. Dies schließt insbesondere die Verwaltung der Softwarequellen und von (kundenspezifischen) Konfigurationen eines Gerätes ein.
Kryptografie	Ausführliche Erläuterungen zum Stand der Technik in der Kryptografie sind im ENISA *Algorithms, Key Sizes and Parameters Report* [6] zu finden.
Kryptografische Hashfunktion	Kryptografische Hashfunktionen müssen sich wie Einwegfunktionen verhalten und sowohl schwach als auch stark kollisions-resistent sein. Veränderungen in der Eingabenachricht müssen zu einer deutlichen Veränderung im Hashwert führen. Beispiel: SHA-256. Siehe auch ENISA [6].
LAN	Local Area Network.
MAC	Nachrichtenauthentifizierungscodes. Dient der Überprüfung der

	Datenintegrität. Beispiele: CMAC, GMAC. Siehe auch ENISA [6].
Monitoring System	Siehe **Intrusion Detection System**.
Multicast	Beim **Multicast** wird die Nachricht zeitgleich an ausgewählte Teilnehmer im Netzwerk gesendet. Spezialfall eines **Broadcasts**.
NESCOR	National Electric Sector Cybersecurity Organization Resource. Programm des US-amerikanischen **EPRI**. Siehe auch [23].
NIST	*National Institute of Standards and Technology.*
Nonce	Eine Nonce ist ein eindeutiger, zufällig erzeugter String, der genau einmal verwendet werden darf (der im mittelalterlichen Englisch gebräuchliche Ausdruck “for the nonce“ bedeutet „für dieses eine Mal“). Wird an Nachricht angehängt, um **Wiedereinspielangriffe** zu erkennen bzw. zu verhindern.
OSI	Open Systems Interconnection. Referenzmodell der Netzwerkkommunikation.
Passwort-authentifizierung	Der Benutzer verwendet Benutzername und Passwort oder PIN, um sich am Gerät einzuloggen. Das Gerät selbst braucht sich nicht zu authentifizieren. Diese Methode ist besonders anfällig gegenüber Ausspähen von Passwörtern mit *Social Engineering* Angriffen. Für kritische Bereiche wird daher **Gegenseitige Authentifizierung** empfohlen.
Penetrationstest	Richtlinien für Penetrationstests werden unter anderem im **EPRI** Programm **NESCOR** als „AMI Penetration Test Plan“ herausgegeben.
Personenbezogene Daten	Siehe Datenschutzverordnung. Beispiel: Lastprofilwerte.
PLC	Power Line Communication.
Produktlebens-zyklus	Der Produktlebenszyklus umfasst die Phasen vom Design, der Entwicklung, der Produktion und Lieferung, des Betriebs und der Dekommissionierung eines Gerätes.
Protokoll	Ereignisse im Zählerbetrieb werden in einer oder mehreren Protokolldateien erfasst. Eine andere Bezeichnung ist auch Logdatei oder Logbuch. Bei einem **rollierenden Protokoll** können Einträge (mit den entsprechenden Berechtigungen) überschrieben werden,

	nachdem der für das Protokoll reservierte Speicherbereich voll ist.
Public-Key Infrastruktur	System mit dem **Zertifikate** ausgestellt, verteilt und verifiziert werden.
Public-Key Kryptografie	Kryptografisches Verfahren, bei dem ein öffentlicher Schlüssel bereitgestellt wird und für **Verschlüsselung** sowie die Verifikation von **digitalen Signaturen** verwendet wird. Zu jedem öffentlichen Schlüssel gehört ein privater Schlüssel, der unter keinen Umständen bekannt gemacht werden darf (also *geheim* gehalten werden muss). Der private Schlüssel dient der Entschlüsselung sowie dem **digitalen Signieren** von Nachrichten. Public-Key Kryptografie werden nicht für die direkte Verschlüsslung von Nachrichten verwendet; vielmehr werden in sogenannten **Hybridverfahren** symmetrische Sitzungsschlüssel unter dem öffentlichen Schlüssel verschlüsselt und versandt. Die Authentizität eines öffentlichen Schlüssels ist mit Zertifikaten in einer **Public-Key Infrastruktur** (PKI) sicherzustellen. Siehe auch ENISA [6]. Das bekannteste Verfahren zur Verschlüsselung ist *RSA*. Prinzipiell ist es möglich mit RSA digital zu signieren; in der Praxis werden **digitale Signaturen** jedoch mit auf elliptischen Kurven (**EC**) basierenden Verfahren erstellt.
Read-Only	Der Nutzer darf Daten lesen. Es dürfen weder neue Daten geschrieben noch vorhandene Daten verändert werden.
Read-Write	Der Nutzer hat Lese- und Schreibrecht.
Replay (Attack)	Siehe **Wiedereinspielangriff**.
RFC	Requests for Comments. Herausgegeben von der **IETF**.
Robustheitstest	Ein Robustheitstest wird zur Qualitätssicherung der Designstabilität des Systems durchgeführt. Hierbei wird insbesondere die Fehlertoleranz getestet.
Rolle	Siehe Kapitel B.3.
Schlüsselmaterial	Der Begriff Schlüsselmaterial beinhaltet alle kryptografischen Schlüssel. Beispiele sind der Master Key, symmetrische Schlüssel, **Sitzungsschlüssel**, private und öffentliche Schlüssel (Public-Key Kryptografie).

Sitzungsschlüssel	Symmetrischer Schlüssel, der für die Verschlüsselung aller Nachrichten innerhalb eines zeitlich begrenzten Zeitraums (Sitzung) verwendet wird.
Spartenzähler	Beispielsweise Zähler für den Gas-, Wasser- oder Wärmeverbrauch.
Unicast	Beim **Unicast** wird die Nachricht an genauen einen Netzwerkteilnehmer gesendet. Siehe auch **Broadcast**.
Unidirektional	Nur in eine Richtung. Siehe auch **Unidirektionale Schnittstelle**.
Unidirektionale Schnittstelle	Bei der Datenübertragung fließen Signale nur in eine Richtung. Beispielsweise nur vom Zähler zum Kunden über die Kundenschnittstelle.
Verschlüsselung	Die Nachricht wird unter Verwendung eines kryptografischen Verfahrens in eine für den Angreifer unlesbare Zeichenfolge (Chiffre) umgewandelt. Entschlüsselung, also die Umwandlung der Chiffre in den ursprünglichen Nachrichtentext, geschieht entweder mit demselben Schlüssel (symmetrisches Verfahren) oder mithilfe des privaten Schlüssels (**Public-Key Kryptografie**).
Versionierung	Versionsverwaltung.
Versionierungs-prozess	Ein **Versionierung**sprozess ist Teil des **Konfigurationsmanagements**.
Vier-Augen Prinzip	Mehrfache Kontrolle. Entscheidung muss von mehr als einer Person getroffen werden.
Vertraulichkeit	Auf vertrauliche Nachrichten dürfen nur bestimmte Kommunikationsteilnehmer zugreifen. Dies geschieht oft durch **Verschlüsselung** der Nachrichten, wobei nur berechtigte Personen Zugang zum geheimen **Schlüsselmaterial** bekommen.
WAN	Wide Area Network.
Wartungs-schnittstelle	Siehe *Kapitel B.*
Wiedereinspiel-angriff	Der Angreifer speichert die Daten einer Sitzung und verwendet diese später, um eine falsche Identität vorzutäuschen. Im Englischen mit **replay attack** bezeichnet.
Zähler	Der Begriff **Zähler** bezieht sich in erster Linie auf den Stromzähler. Falls notwendig, wird explizit zwischen **Stromzähler**

	und **Spartenzähler** unterschieden.
Zertifikat	Ein digitales Zertifikat ist eine Datei, die die Überprüfung der **Authentizität** eines Kommunikationsteilnehmers oder einer Nachricht ermöglicht. Siehe **Public-Key Infrastuktur**.

Anhang C Verwendete Richtlinien und Referenzen

[1] E-Control Austria. *Risikoanalyse für die Informationssysteme der Elektrizitätswirtschaft*, 27.Februar 2014. https://www.e-control.at/publikationen/publikationen-strom/studien/ikt-risikoanalyse(zuletzt abgerufen am 31. Oktober 2017)

[2] Bundesamt für Sicherheit in der Informationstechnik. TR-03109-1. *Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems.* Version 1.0, Bonn, Deutschland, März 2013.

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

[4] National Institute of Standards and Technology. Special Publication 800-57 Part 1 Rev. 4, *Recommendation for Key Management*, Januar 2016.

[5] Bundesamt für Sicherheit in der Informationstechnik. TR-03116, Teil 3, *Kryptographische Vorgaben für Projekte der Bundesregierung – Intelligente Messsysteme*. Wird jährlich angepasst. Bonn, Deutschland, Stand: 2017.

[6] Bundesamt für Sicherheit in der Informationstechnik. TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen. Version: 2017-01. Bonn, Deutschland, Februar 2017

[7] National Institute of Standards and Technology. Special Publication 800-38D. *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*. November 2007.

[8] Internet Engineering Task Force. *RFC 5114: Additional Diffie-Hellman Groups for Use with IETF Standards*, 2008. http://www.ietf.org/rfc/rfc5114.txt

[9] Bundesamt für Sicherheit in der Informationstechnik. ECC Brainpool. *ECC Brainpool Standard Curves and Curve Generation*. Version 1.0 (2005), Bonn, Deutschland, http://www.ecc-brainpool.org (zuletzt abgerufen am 31. November 2017)

[10] Internet Engineering Task Force. *RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2*, 2008. http://www.ietf.org/rfc/rfc5246.txt

[11] Internet Engineering Task Force. *RFC 5289: TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)*, 2008. http://www.ietf.org/rfc/rfc5289.txt

[12] National Institute of Standards and Technology. *FIPS PUB 186-2, Digital Signature Standard (DSS)*, 2000.

[13] National Institute of Standards and Technology. *FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, Mai 2001.

[14] National Institute of Standards and Technology. *Annex C: Approved Random Number Generators for FIPS PUB 140-2* [13], Februar 2012.

[15] Bundesamt für Sicherheit in der Informationstechnik:: *Anwendungshinweise und Interpretationen zum Schema, AIS 20*, *Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren*, Version 3.0, Bonn, Deutschland, Mai 2013.

[16] Bundesamt für Sicherheit in der Informationstechnik: *Anwendungshinweise und Interpretationen zum Schema, AIS 31, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren*, Version 3.0, Bonn, Deutschland, Mai 2013.

[17] National Institute of Standards and Technology. *Cryptographic Algorithm Validation Program*. http://csrc.nist.gov/groups/STM/cavp/(zuletzt abgerufen am 31. Oktober 2017)

[18] ÖNORM A 7700. *Sicherheitstechnische Anforderungen an Webapplikationen*. 2008.

[19] Open Web Application Security Project. https://www.owasp.org/index.php/Data_Validation (zuletzt abgerufen am 31. Oktober 2017)

[20] *RSA. PKCS #11: Cryptographic Token Interface Standard.* Zu Aktualisierungen siehe OASIS https://www.oasis-open.org/standards (zuletzt abgerufen am 31. Oktober 2017).

[21] Internet Engineering Task Force. *PKCS #5: Password-Based Cryptography Specification Version 2.0*, 2000. http://tools.ietf.org/rfc/rfc2898.txt

[22] Ari Takanen, Jared DeMott, and Charlie Miller. *Fuzzing for Software Security Testing and Quality Assurance* (1 ed.). Artech House, Inc., Norwood, MA, USA, 2008.

[23] Electric Power Research Institute. *National Electric Sector Cybersecurity Organization Resource*. http://smartgrid.epri.com/NESCOR.aspx (zuletzt abgerufen am 31. Oktober 2017)