

DIN CEN/CLC/TS 17880

ICS 33.200; 35.030; 35.240.99

**Schutzprofil für Smart Meter –
Mindestsicherheitsanforderungen;
Deutsche Fassung CEN/CLC/TS 17880:2022**

Protection Profile for Smart Meter –
Minimum Security requirements;
German version CEN/CLC/TS 17880:2022

Gesamtumfang 84 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (CEN/CLC/TS 17880:2022) wurde vom Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige deutsche Normungsgremium ist der Arbeitskreis NA 043-04-27-04 AK „IT-Sicherheitsmaßnahmen und Dienste“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Technische Spezifikationen sind nicht Bestandteil des Deutschen Normenwerks.

Diese Technische Spezifikation ist das Ergebnis einer Normungsarbeit, das mit Rücksicht auf die europäischen Rahmenbedingungen von DIN nicht als Norm herausgegeben wird.

Zur vorliegenden Technischen Spezifikation wurde kein Entwurf veröffentlicht.

Erfahrungen mit dieser Technischen Spezifikation sind erbeten:

- vorzugsweise als Datei per E-Mail an nia@din.de in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin.

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO/IEC 15408-1	siehe	DIN EN ISO/IEC 15408-1
ISO/IEC 15408-2	siehe	DIN EN ISO/IEC 15408-2
ISO/IEC 15408-3	siehe	DIN EN ISO/IEC 15408-3
ISO/IEC 18045	siehe	DIN EN ISO/IEC 18045

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN EN ISO/IEC 15408-1, *Informationstechnik — IT-Sicherheitsverfahren — Evaluationskriterien für IT-Sicherheit — Teil 1: Einführung und allgemeines Modell*

DIN EN ISO/IEC 15408-2, *Informationstechnik — IT-Sicherheitsverfahren — Evaluationskriterien für IT-Sicherheit — Teil 2: Sicherheitsfunktionskomponenten*

DIN EN ISO/IEC 15408-3, *Informationstechnik — IT-Sicherheitsverfahren — Evaluationskriterien für IT-Sicherheit — Teil 3: Komponenten zur Sicherheitskontrolle*

DIN EN ISO/IEC 18045, *Informationstechnik — Sicherheitstechniken — Methodik für die Bewertung der IT-Sicherheit*

— Leerseite —

Deutsche Fassung

Schutzprofil für Smart Meter — Mindestsicherheitsanforderungen

Protection Profile for Smart Meter —
Minimum Security requirements

Diese Technische Spezifikation (CEN/TS) wurde vom CEN am 4. Dezember 2022 als eine künftige Norm zur vorläufigen Anwendung angenommen.

Die Gültigkeitsdauer dieser CEN/TS ist zunächst auf drei Jahre begrenzt. Nach zwei Jahren werden die Mitglieder von CEN und CENELEC gebeten, ihre Stellungnahmen abzugeben, insbesondere über die Frage, ob die CEN/TS in eine Europäische Norm umgewandelt werden kann.

Die CEN- und CENELEC-Mitglieder sind verpflichtet, das Vorhandensein dieser CEN/TS in der gleichen Weise wie bei einer EN anzukündigen und die CEN/TS verfügbar zu machen. Es ist zulässig, entgegenstehende nationale Normen bis zur Entscheidung über eine mögliche Umwandlung der CEN/TS in eine EN (parallel zur CEN/TS) beizubehalten.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.



CEN-CENELEC Management-Zentrum:
Rue de la Science 23, B-1040 Brüssel

Inhalt

	Seite
Europäisches Vorwort	4
Einleitung	5
1 Anwendungsbereich.....	6
2 Normative Verweisungen	6
3 Begriffe	6
4 Evaluierungsgegenstand.....	10
5 Konformitätsansprüche	12
6 Definition des Sicherheitsproblems	12
6.1 Werte.....	12
6.2 Entitäten und Bedrohungsagenten	13
6.3 Bedrohungen.....	13
6.3.1 Allgemeines	13
6.3.2 T.NetworkDisclosure - Unbefugte Datenoffenlegung durch Netzzugang.....	13
6.3.3 T.DirectDisclosure - Unbefugte Datenoffenlegung durch Direktzugang.....	13
6.3.4 T.NetworkDataMod - Unbefugte Datenveränderung durch Netzzugang	14
6.3.5 T.DirectDataMod - Unbefugte Datenveränderung durch Direktzugang	14
6.3.6 T.Malfunction - Gefährdung von Werten aufgrund einer Fehlfunktion des TOE	14
6.4 Organisatorische Sicherheitsrichtlinien.....	14
6.4.1 Allgemeines	14
6.4.2 P.Logging - Protokollierung von Sicherheitsereignissen.....	14
6.4.3 P.Alarms - Alarmierung bei kritischen Ereignissen.....	15
6.5 Annahmen	15
6.5.1 A.ExternalData - Schutz von Daten außerhalb der TOE-Steuerung	15
6.5.2 A.AuditSupport - Überprüfung der Auditdaten	15
6.5.3 A.InspectionSupport - Prüfung der Integrität von Zählern	15
6.5.4 A.UniqueSubjectIDs - Subjekte haben eindeutige Identifikationsschlüssel.....	15
7 Sicherheitszielsetzungen	16
7.1 Allgemeines	16
7.2 Sicherheitszielsetzungen für den TOE	16
7.2.1 Allgemeines	16
7.2.2 O.Authorization - Berechtigung für den Zugriff auf TOE-Daten und -Funktionen	16
7.2.3 O.Messages - Nachrichtenschutz	16
7.2.4 O.DataAtRest - Schutz gespeicherter Daten	16
7.2.5 O.Crypto - Zugelassene kryptographische Mechanismen	16
7.2.6 O.Interfaces - Nicht-operative Schnittstellen deaktiviert	17
7.2.7 O.Resilience - Resilienz gegen Ausfälle	17
7.2.8 O.SecureUpdate - Durch digitale Signatur geschützte Updates	17
7.2.9 O.Logging - Protokollierung von Sicherheitsereignissen.....	17
7.2.10 O.Alarms - Alarme für kritische Ereignisse.....	17
7.3 Sicherheitszielsetzungen für die Operative Umgebung	17
7.3.1 OE.ExternalData - Schutz von Daten außerhalb der TOE-Steuerung	17
7.3.2 OE.AuditSupport - Überprüfung der Auditdaten.....	17
7.3.3 OE.InspectionSupport - Prüfungen der Integrität von Zählern	17
7.3.4 OE.UniqueSubjectIDs - Subjekte haben eindeutige Identifikationsschlüssel	18

8	Erweiterte Definitionen der Komponenten.....	18
8.1	Allgemeines	18
8.2	Alarm bei Sicherheitsereignissen (FAU_ARP.2)	18
8.3	Vertrauenswürdige Software-Update (FPT_TSU.1)	19
8.4	Grundlegende TSF-Selbstprüfung (FPT_BST.1).....	20
8.5	Manipulationsmeldung (FPT_TNN.1).....	21
8.6	Generierung von Zufallszahlen (FCS_RNG.1).....	22
8.6.1	Verhalten der Familie	22
9	Sicherheitsanforderungen	23
9.1	Typographische Konventionen	23
9.2	SFR-Architektur	23
9.3	Funktionale Sicherheitsanforderungen.....	26
9.3.1	Kryptographische Unterstützung.....	26
9.3.2	Schutz der Benutzerdaten.....	29
9.3.3	Identifizierung und Authentifizierung.....	37
9.3.4	Schutz der TSF	39
9.3.5	Sicherheitsmanagement	42
9.3.6	Sicherheitsaudit.....	45
9.4	Sicherheitsgewährleistungsanforderungen.....	50
9.4.1	Präzisierungen der Sicherheitsgewährleistungsanforderungen	51
10	Begründungen	59
10.1	Begründung für die Sicherheitszielsetzungen.....	59
10.1.1	Abdeckung der Sicherheitszielsetzungen	59
10.1.2	Angemessene Sicherheitszielsetzungen	60
10.2	Begründung für die Sicherheitsanforderungen.....	61
10.2.1	Abdeckung der Sicherheitsanforderungen.....	61
10.2.2	SFR-Abhängigkeiten	65
10.2.3	Begründung für SARs	68
Anhang A (informativ) Zuordnung zu Mindestsicherheitsanforderungen		69
Literaturhinweise.....		80

Europäisches Vorwort

Dieses Dokument (CEN/CLC/TS 17880:2022) wurde vom Technischen Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ erarbeitet, dessen Sekretariat von DIN gehalten wird.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Grundlage ist das von der CEN/CENELEC/ETSI Koordinationsgruppe für Smart Meter (CG-SM) erstellte „Schutzprofil für die Mindestsicherheitsanforderungen an Smart Meter“ Version 1.0, 30. Oktober 2019 (CENCLCETSI_SMCG/Sec/00156/DC).

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Liste dieser Institute ist auf den Internetseiten von CEN abrufbar.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Technische Spezifikation anzukündigen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Einleitung

Dieses Schutzprofil beschreibt eine Reihe von Sicherheitsanforderungen an Smart Meter, die auf den „Mindestsicherheitsanforderungen“ für Komponenten von erweiterten Messinfrastrukturen aufbauen. Die Anforderungen im Datenschutz- und Sicherheitskonzept der Koordinationsgruppe für Smart Meter - Teil IV basieren auf dem Konzept, dass es eine gemeinsame/generische Reihe von zugrundeliegenden „Mindest“-Sicherheitsanforderungen gibt, die mit den Spezifikationen der Smart Metering-Anforderungen in einer Reihe von EU-Mitgliedstaaten verbunden sind. Die Mitglieder des Ad-hoc-CG-SM-Arbeitskreises für Datenschutz und Sicherheit haben daraufhin eine Reihe allgemeiner Mindestanforderungen entwickelt, die für die meisten europäischen Mitgliedstaaten gelten. Aus dieser Reihe wurden dann die Anforderungen, die auf Smart Meter (im Gegensatz zu anderen Teilen der AMI) anwendbar sind, als Grundlage für das vorliegende Schutzprofil verwendet, indem sie in funktionale Sicherheitsanforderungen der Common Criteria (en: Security Functional Requirements, SFRs) und Präzisierungen der Sicherheitsgewährleistungsanforderungen (en: Security Assurance Requirements, SARs) umgesetzt wurden.¹ Die in diesem Schutzprofil definierten Anforderungen können daher als Grundlage für spezifische Anforderungen der einzelnen EU-Mitgliedstaaten dienen, die auf einer Risikoanalyse beruhen, bei der die für ihr System geltenden spezifischen Werte und Akteure beurteilt wurden.

Ziel dieses Schutzprofils ist es, einen europäischen Ansatz für die Sicherheitszertifizierung von Smart Metern zu finden. Das im Juni 2019 in Kraft getretene Cybersicherheitsgesetz der Europäischen Kommission fordert die Entwicklung von europäischen Zertifizierungssystemen für Produkte, Prozesse und Dienste, um eine Fragmentierung des Marktes durch verschiedene nationale Zertifizierungssysteme zu verhindern. Der Arbeitskreis Datenschutz und Sicherheit der SM-CG ist der Meinung, dass die Common Criteria ein kostengünstiges und effizientes Verfahren für eine Vereinbarung zwischen Herstellern, Kunden und Sicherheitsevaluatoren darüber darstellen, welche Vertrauenswürdigkeitsstufe ein Produkt auf der Grundlage eines Schutzprofils und von Sicherheitsvorgaben für Smart Meter aufweisen muss.

Der Arbeitskreis erkennt an, dass es bereits einige nationale Systeme gibt, die sich bewährt haben, wie z. B. das französische CSPN-Konzept (fr: Certification Sécurité de Premier Niveau) oder das CPA-Konzept (en: Commercial Product Assurance) in Großbritannien, und ist der Ansicht, dass es möglich sein muss, diese nationalen Konzepte fortzuführen. Parallel dazu ist der Arbeitskreis der Ansicht, dass ein Ansatz, der auf den Common Criteria EAL3+ und der bereits bestehenden gegenseitigen Anerkennung von CC-Zertifikaten zwischen 17 europäischen Ländern basiert, eine wertvolle Alternative für europäische Länder darstellt, die noch kein Zertifizierungssystem für Smart Meter haben.

Der Inhalt eines Schutzprofils ist in ISO/IEC 15408-1 definiert.

Abschnitt 4 bis Abschnitt 7 basieren auf allgemeinen Konzepten – sie sind daher für ein breites Publikum gedacht. Andere Abschnitte enthalten detailliertere Anforderungen und verlangen eine gewisse Vertrautheit mit den Konzepten der Common Criteria in ISO/IEC 15408 (alle Teile). Diese detaillierteren Anforderungen werden von den Common-Criteria-Experten in den Entwicklerorganisationen verwendet, wenn sie eine Sicherheitsvorgabe (en: Security Target, ST) schreiben, die die Konformität mit diesem Schutzprofil für ihr Produkt beansprucht und die produktspezifische Art und Weise aufzeigt, in der die Anforderungen erfüllt und in dem Produkt umgesetzt werden. Während der Evaluierung des Produkts überprüfen die Evaluatoren die Konformität der ST des Entwicklers mit diesem Schutzprofil sowie die Konformität des Produkts mit den Anforderungen in den ST.

Jede Sicherheitsfunktion des Zählers ist eine zusätzliche Funktion, die keinen Einfluss auf die messtechnischen Eigenschaften des Zählers hat.

¹ Im Allgemeinen werden die Anforderungen an die Vertrauenswürdigkeit präzisiert, um die erforderlichen Evaluierungsaufgaben klarer zu definieren und die Konsistenz der Evaluierungen anhand der Anforderungen in diesem Schutzprofil zu verbessern.

1 Anwendungsbereich

Dieses Dokument spezifiziert einen Sicherheitszertifizierungsansatz für intelligente Stromzähler (Smart Electricity Meter). Sie bietet eine allgemeine Lösung für die Sicherheitszertifizierung, um eine Fragmentierung zu vermeiden und die gegenseitige Anerkennung von Zertifikaten in Europa zu ermöglichen. Sie definiert die funktionalen Anforderungen und Vertrauenswürdigkeitskriterien (siehe die Gemeinsamen Kriterien in ISO/IEC 15408 (alle Teile)) für die Sicherheitszertifizierung.

In diesem Schutzprofil werden keine spezifischen Arten von sensiblen personenbezogenen Daten oder persönlich identifizierbaren Informationen definiert.

2 Normative Verweisungen

Es gibt keine normativen Verweisungen in diesem Dokument.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <https://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>

3.1 Administrator
Rolle, die in Bezug auf alle von der TSF umgesetzten Richtlinien ein gewisses Maß an Vertrauen genießt im Sinne eines allgemeinen Begriffs für eine privilegierte Rolle, die Zugang zu sensiblen die Konfiguration und den Betrieb des Zählers betreffenden Vorgängen hat

3.2 Advanced Metering Infrastructure
Infrastruktur, die eine bidirektionale Kommunikation zwischen dem Head End System und dem/den Zähler(n) ermöglicht

Anmerkung zum Begriff: Eine Advanced Metering Infrastructure kann auch mit anderen Geräten im Haus verbunden werden.

3.3 Vertrauenswürdigkeit
Gründe für das Vertrauen, dass ein TOE die SFRs erfüllt

3.4 Verbraucher
Endverbraucher der gemessenen Menge (Strom, Gas, Wasser oder Wärmeenergie)

3.5 kritisches Ereignis
Ereignis, das in einem Smart Meter eintreten kann und das für die Versorgung oder die Sicherheit des Zählers von besonderer Bedeutung ist

Anmerkung 1 zum Begriff: Die kritischen Ereignisse für einen mit diesem Schutzprofil konformen Zähler sind als Teil von FAU_ARP.2 in 9.3.6.1 definiert.)

3.6

digitale Signatur

kryptographische Techniken, die auf Daten angewendet werden, um deren Integrität und Authentizität zu überprüfen

3.7

direkte Schnittstelle

Schnittstelle zum Zähler, die keinen Zugriff von externen Netzen beinhaltet

Anmerkung 1 zum Begriff: Bei den externen Netzen kann es sich um WAN, Nachbarschaftsnetze oder lokale Netze handeln.

3.8

elektromagnetisch

EM

physikalische Eigenschaft, die mit der Wechselbeziehung zwischen elektrischen Strömen oder Feldern und Magnetfeldern zusammenhängt

3.9

Evaluator

Person oder Gruppe, die eine Sicherheitsbewertung des TOE durchführt

Anmerkung 1 zum Begriff: Ein Beispiel für eine Evaluierungsnorm ist ISO/IEC 15408-3 mit der zugehörigen Methodik für die Bewertung, die in ISO/IEC 18045 beschrieben ist.

3.10

Firmware

ausführbarer Code eines Zählers, der in der Hardware gespeichert ist

Anmerkung 1 zum Begriff: Für die Zwecke dieses Schutzprofils ist das entsprechende Aktualisierungsverfahren in FPT_TSU.1 definiert, siehe 9.3.4.6.

3.11

handgehaltenes Endgerät

tragbares Gerät zum Ablesen und Programmieren von Geräten oder Zählern in den Räumlichkeiten des Verbrauchers oder an der Zugangsstelle

3.12

Joint Test Action Group

JTAG

häufig verwendetes Synonym für die im IEEE-Standard 1149.1 definierte Schnittstelle zum Testen digitaler Bausteine (Standard Test Access Port und Boundary-Scan Architecture)

3.13

lokales Netz

Datenkommunikationsnetz, das Zugang zu lokalen (hausinternen/gebäudeeigenen) Geräten und/oder anderen lokalen Netzen bietet

3.14

Nachrichtenauthentisierungscode

MAC, en: message authentication code

kryptographische Prüfsumme über Nachrichtendaten, die verwendet wird, um sicherzustellen, dass der Absender einer Nachricht derjenige ist, der er vorgibt zu sein, und dass die Nachricht in der ursprünglich gesendeten Form vorliegt (unter der Annahme, dass ein kryptographischer Schlüssel nur dem Absender und dem Empfänger bekannt ist)

3.15

Nachricht

Kommunikation auf Anwendungsebene, die an einen Empfänger gesendet oder für ihn hinterlassen wird

Anmerkung 1 zum Begriff: Die Mindestanforderungen im Datenschutz- und Sicherheitskonzept der Koordinationsgruppe für Smart Meter – Teil IV, v1.1, 17. Juli 2016, die die Quelle für dieses Schutzprofil sind, beinhalten, dass die Sicherheit auf der Anwendungsebene implementiert wird, unabhängig von den Schutzmaßnahmen, die das Kommunikationsprotokoll bieten könnte.

3.16

Zählerdaten

Zählerstände, die die Berechnung der in einer bestimmten Zeitspanne verbrauchten Menge an Strom, Gas, Wasser oder Wärmeenergie ermöglichen

Anmerkung 1 zum Begriff: Die Zählerdaten können somit tägliche und monatliche Zählerstände, Intervallablesungen und Istwerte des Zählerstands umfassen. Andere Messwerte und Daten dürfen ebenfalls einbezogen werden (z. B. Qualitätsdaten, Ereignisse und Alarme).

3.17

Metrologie

Nicht-TSF-Teil des TOE, der eine physikalische Eigenschaft in ein digitales Signal umwandelt. Diese Funktionen werden durch die Anforderungen der Messgeräte-richtlinie 2004/22/EG (MID, en: Measuring Instruments Directive) geregelt

3.18

Nachbarschaftsnetz

Datenkommunikationsnetz, das Zugang zu mehreren Gebäuden und/oder anderen Nachbarschaftsnetzen bietet

3.19

operative Schnittstellen

Schnittstellen, die für den normalen Betrieb des Messgeräts erforderlich sind (alle anderen zugänglichen Schnittstellen sind deaktiviert)

3.20

Schutzprofil

PP, en: protection profile

implementierungsunabhängige Beschreibung der Sicherheitsanforderungen für einen TOE-Typ

[QUELLE: ISO/IEC 15408-1:2009, 3.1.52]

3.21

Rolle

Berechtigung einer Partei, einen Satz von einem oder mehreren Befehlen auszuführen, die mit dem Rollennamen verbunden sind

3.22

Sicherheitsgewährleistungsanforderung

SAR, en: security assurance requirement

Beschreibung, wie der TOE unter Verwendung der standardisierten Sprache zu evaluieren ist

3.23

funktionale Sicherheitsanforderung

SFR, en: security functional requirement

Umwandlung der Sicherheitszielsetzungen für den TOE in eine Reihe von standardisierten funktionalen Anforderungen

Anmerkung 1 zum Begriff: Die SFR für das PP sind der ISO/IEC 15408-2 entnommen (oder als erweiterte Komponenten in Abschnitt 8 definiert).

3.24

Sensor

Gerät, das eine physikalische Eigenschaft in ein elektrisches Signal umwandelt

Anmerkung 1 zum Begriff: Ein Sensor kann ein Nicht-TSF-Teil des TOE sein oder extern verbaut werden.

BEISPIEL Ein Stromwandler oder ein Temperaturfühler an einer Wasserrücklaufleitung.

3.25

Servicetechniker

Benutzer, die lokale Installations-, Inbetriebnahme-, Wartungs- oder Diagnosetätigkeiten an einem Messgerät durchführen

Anmerkung 1 zum Begriff: Diese Tätigkeiten dürfen über direkte oder Netzschnittstellen ausgeführt werden, und Servicetechniker benötigen möglicherweise Zugang zu privilegierten Funktionen.

3.26

Koordinationsgruppe für Smart Meter

SM-CG, en: smart meters co-ordination group

gemeinsames Beratungsgremium, das Fachwissen und Ressourcen der europäischen Normungsorganisationen (CEN, CENELEC und ETSI) bündelt und eine zentrale Anlaufstelle für Fragen der Normung im Bereich der intelligenten Verbrauchsmessung darstellt

3.27

Sicherheitsvorgabe

ST, en: security target

implementierungsabhängige Beschreibung der Sicherheitsanforderungen für einen spezifischen, identifizierten TOE

[QUELLE: ISO/IEC 15408-1:2009, 3.1.63]

3.28

Evaluierungsgegenstand

TOE, en: target of evaluation

Satz von Software, Firmware und/oder Hardware, möglicherweise mit beigefügten Leitlinien

[QUELLE: ISO/IEC 15408-1:2009, 3.1.70, modifiziert]

3.29

TOE-Sicherheitsfunktionalität

TSF, en: TOE security functionality

kombinierte Funktionalität der gesamten Hardware, Software und Firmware eines TOE (3.3.4), welche die korrekte Durchsetzung der SFRs (3.3.7) sicherstellen muss

[QUELLE: ISO/IEC 15408-1:2009, 3.1.74]

3.30

TSF-Daten

Daten für den Betrieb des TOE, welche für die Durchsetzung des SFR benötigt werden

[QUELLE: ISO/IEC 15408-1:2009, 3.1.81]

3.31

Benutzer

externe Entität

menschliche oder IT-Entität, die mit dem TOE von außerhalb der TOE-Grenze interagiert

3.32

Weitverkehrsnetz

WAN, en: Wide Area Network

ausgedehntes Datenkommunikationsnetz, das eine große Anzahl von Kommunikationsgeräten in einem großen geographischen Gebiet verbindet

4 Evaluierungsgegenstand

Der Evaluierungsgegenstand (TOE) ist ein intelligenter Versorgungszähler, der den Verbrauch von Strom, Gas, thermischer Energie oder Wasser², die von Versorgungsmärkten bereitgestellt werden, überwacht und möglicherweise begrenzt und mit den Benutzern sowohl über lokale („direkte“) als auch über Netzchnittstellen kommuniziert. Bild 1 zeigt die generische Architektur des TOE. (Die Schnittstellen sind auch mit „C“, „G1“, „H1“ und „M“ gekennzeichnet, um die Übereinstimmung mit CEN/CLC/ETSI TR 50571 zu zeigen.)

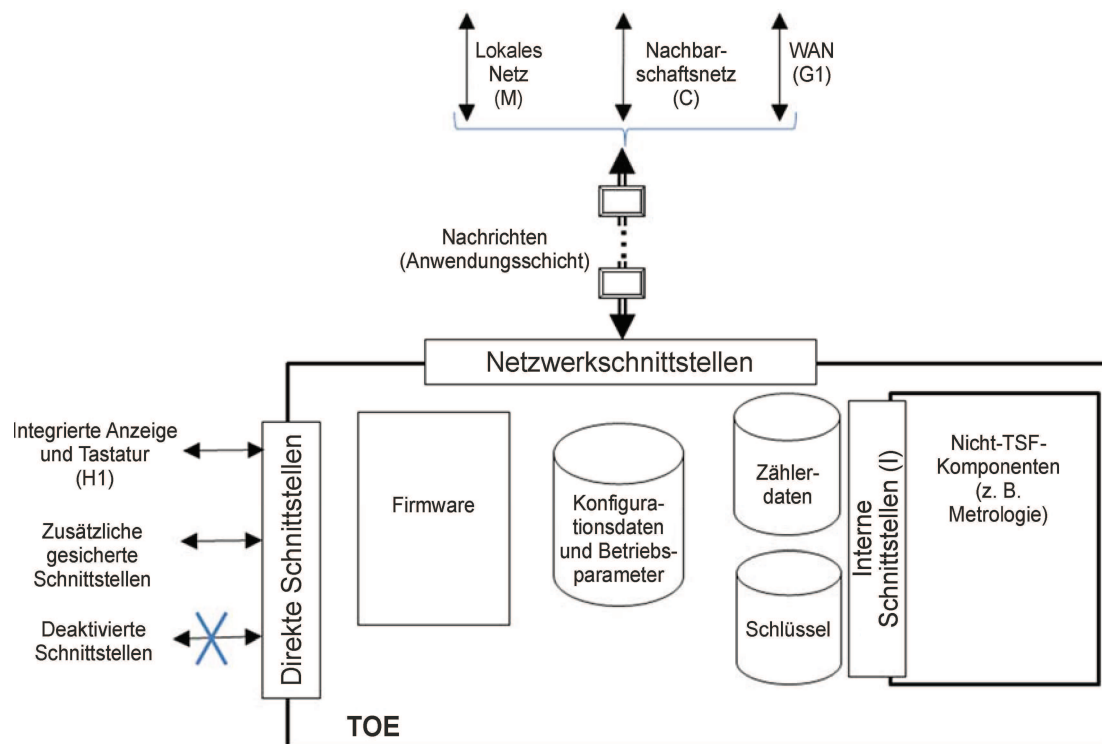


Bild 1 — Generische Architektur des TOE für Smart Meter

Der TOE bietet eine Kombination der folgenden zählerbezogenen Funktionen aus der Referenzarchitektur in [1]:

- Auflistung der messtechnischen Funktionen einschließlich der konventionellen Zähleranzeige (Register oder Index), die der gesetzlichen messtechnischen Kontrolle unterliegen. Wenn sie messtechnisch

² Erschöpfende Liste, die den wichtigsten Medientypen im OBIS-Kennzeichnungssystem entspricht.

kontrolliert werden, unterliegen diese Funktionen den Anforderungen der Richtlinie 2004/22/EG über Messgeräte (MID)

- zusätzliche Funktionen, die nicht von der MID abgedeckt werden, wie z. B. die Fernablesung des Zählers, fortschrittliche Tarif- und Zahlungssysteme sowie die Fernfreigabe und -sperrung der Versorgung.
- Zählerkommunikationsfunktionen, einschließlich Netzschnittstellen und Direktschnittstellen.

Alle Smart Meter, die diesem PP entsprechen, implementieren Messfunktionen, einige zusätzliche Funktionen und Kommunikationsfunktionen. Allerdings werden nicht alle Zähler die gleichen zusätzlichen Funktionen implementieren und auch nicht unbedingt alle Kommunikationsschnittstellen unterstützen. Dieses PP befasst sich diesbezüglich mit den Unbekannten, indem es die Identifizierung der TOE-spezifischen Details in einem ST verlangt, der diesem PP entspricht, und indem es Präzisierungen bestimmter SARs definiert, um Konsistenzprüfungen für zählerspezifische Details zu unterstützen.

Die grundlegende Sicherheitsaufgabe des Zählers besteht darin, die Integrität seines Inhalts, die Authentizität und Integrität der Anweisungen, auf die es reagiert, sowie die Vertraulichkeit der Daten, die zur Bereitstellung dieser anderen Sicherheitsinformationen verwendet werden, und der personenbezogenen Daten sicherzustellen. Ein Großteil dieser Aufgabe bezieht sich daher auf die Richtlinien, die der Zähler für die Kommunikation über seine verschiedenen Schnittstellen anwendet.

Der Zähler verfügt über eine Reservestromquelle, um die Uhrzeit bei Stromausfällen zu erhalten.

Für die Zwecke dieses PP werden alle Netzschnittstellen einfach so behandelt, als ob sie Nachrichten verschiedener Art mit dem TOE austauschen. Obwohl verschiedene Schnittstellen unterschiedliche Transport- und Anwendungsprotokolle verwenden könnten, erfordert dieses PP, dass alle Netzschnittstellen einer Berechtigungskontrolle auf Nachrichtenebene unterliegen (d. h., dass die Berechtigung, auf den Inhalt einer Nachricht einzuwirken, auf der Nachricht selbst und möglicherweise auf kontextbezogenen Faktoren wie einem authentifizierten logischen End-to-End-Kanal basiert, der zur Übermittlung der Nachrichten verwendet wird).

Die direkten Schnittstellen dürfen ein Display und ein Tastenfeld für die Interaktion mit dem Benutzer sowie andere Kommunikationsschnittstellen in Übereinstimmung mit CEN/CLC/ETSI TR 50571 umfassen. Diese direkten Schnittstellen könnten für die Kommunikation mit anderen Geräten im Haus verwendet werden, z. B. für die Anzeige und Analyse von Verbrauchsdaten, für die Kommunikation mit anderen Zählern oder für die Kommunikation mit Technik- und Wartungswerkzeugen wie z. B. einem handgehaltenen Endgerät.

Ein Zähler darf über eine Reihe von Schnittstellen verfügen, die zum Zeitpunkt der Inbetriebnahme deaktiviert sind (z. B. Schnittstellen für Initialisierung, Installation oder Fehlersuche). Diese Schnittstellen können physisch am Zähler vorhanden sein (z. B. ein optischer Anschluss oder eine Debug-Schnittstelle) oder rein logische Schnittstellen sein (z. B. Technik- oder Wartungsfunktionen über das Display und das Tastenfeld). Dieses PP verlangt, dass die erfolgreiche Deaktivierung dieser Schnittstellen evaluiert wird, um zu bestätigen, dass sie keine Verfahren zur Umgehung der für andere Schnittstellen geltenden Sicherheitsvorschriften während der betrieblichen Nutzung bieten.

Die Zähler-Firmware ist durch eine Firmware-Integritätsprüfung und ein sicheres Aktualisierungsverfahren mit digital signierten Updates, die authentifiziert werden können und deren Integrität zwischen dem Urheber und dem Zähler gesichert ist, vor Manipulationen geschützt. Ein Zähler, der mit diesem PP konform ist, lässt keine Aktualisierung der TOE-Firmware zu, die nicht über den sicheren Aktualisierungsprozess erfolgt.

5 Konformitätsansprüche

Dieses Schutzprofil (PP) entspricht der *ISO/IEC 15408* (alle Teile), sowohl was den Inhalt als auch was die Darstellung betrifft.

Alle funktionalen und sicherheitstechnischen Anforderungen an die Vertrauenswürdigkeit, die in diesem PP festgelegt sind, entsprechen der *ISO/IEC 15408*, Teil 2 bzw. *ISO/IEC 15408*, Teil 3, der oben genannten Common-Criteria-Version.

Dieses PP erhebt keinen Anspruch auf Konformität mit anderen PP. Die Anforderung an die Vertrauenswürdigkeit dieses Schutzprofils entspricht EAL3, ergänzt durch ALC_FLR.3. Dieses Schutzprofil erfordert die strikte Einhaltung aller Sicherheitsvorgaben oder Schutzprofile, die den Anspruch auf Konformität mit diesem Schutzprofil erheben.

6 Definition des Sicherheitsproblems

6.1 Werte

Bei den Werten, die durch den TOE geschützt werden müssen, handelt es sich um verschiedene Arten von Daten, darunter Zählerdaten, Konfigurationsdaten oder andere Betriebsparameter. Fast alle zu erwartenden Vorteile für einen Angreifer ergeben sich aus dem Zugriff auf eine oder mehrere dieser Arten von Daten – z. B. könnte ein Angreifer davon profitieren, dass er das verfügbare Guthaben ändert, dass er die vom TOE gespeicherten oder gesendeten Verbrauchsdaten ändert oder dass er einen Schlüssel erhält, der den Zugriff auf diese Daten ermöglicht. Die Datenarten werden nicht gesondert definiert, da der Zugriff auf alle Daten in der Regel über eine der Direkt- oder Netzwerkschnittstellen des Zählers erfolgt, so dass der Schwerpunkt der Bedrohungen einfach auf dem unbefugten Zugriff auf alle verfügbaren Daten liegt.³

Eine solche Definition erfolgt als Teil der Beschreibung eines spezifischen Systems für den Betrieb eines Messsystems, zu dem der Smart Meter gehört, und/oder in Bezug auf die spezifischen Daten, die von einem bestimmten Zählertyp gespeichert und verarbeitet werden. Kryptographische Schlüssel und Zertifikate eines öffentlichen Schlüssels sind ein Beispiel für Daten, die in diesem PP nicht ausdrücklich genannt werden: Es werden keine bestimmten kryptographischen Systeme oder Mechanismen vorausgesetzt. Die Sicherheitsvorgaben für ein bestimmtes Produkt müssen jedoch die relevanten Parameter mittels ihrer Regeln für die Kontrolle des Zugriffs auf die Konfiguration der Betriebsparameter und ihre Regeln für die Sicherstellung der Nachrichtensicherheit und der Zugriffskontrolle identifizieren. Für die Zwecke dieses Schutzprofils sind die Regeln aufzunehmen zur Wahrung der Vertraulichkeit, Integrität und Authentizität solcher Informationen in die spezifischen Regeln für die Autorisierung, Zugriffskontrolle und Datenvernichtung, die in einer Sicherheitsvorgabe festgelegt sind, aufgenommen werden.⁴

Ein weiteres mögliches Ziel eines Angreifers besteht darin, die Energieversorgung, die der Zähler reguliert, aus der Ferne zu deaktivieren. Dies könnte durch einen unbefugten Zugriff auf Daten wie oben geschehen (z. B. durch Änderung des Saldos eines Vorauszahlungszählers auf einen Wert, bei dem der Zähler die Versorgung unterbricht, oder durch Senden eines Befehls, der den Betriebszustand „Versorgung freigeben/unterbrechen“ ändert). Die Fernsperrung eines Zählers könnte alternativ auch durch die Verursachung eines nicht behebbaren Fehlers im Zähler erreicht werden, weshalb der ordnungsgemäße Betrieb des Zählers in diesem Schutzprofil ebenfalls als Wert behandelt wird.

³ Verschiedene Arten von Zählern dürfen spezifische Richtlinien anwenden, die verschiedene Arten von Daten unterscheiden; in diesem Fall muss dies in den Sicherheitsvorgaben durch die Ergänzung der Regeln in FDP_ACF.1 und FDP_IPF.1/Msgrs sichtbar sein.

⁴ Die Zugangssteuerungsregeln sind in FDP_ACF.1, die Regeln für die Berechtigung in FDP_IPF.1/Msgrs und die Daten, die einer besonderen sicheren Vernichtung unterliegen, in FDP_RIP.1 beschrieben.

6.2 Entitäten und Bedrohungsagenten

Die externen Entitäten, die mit dem TOE interagieren, sind folgende:

Direktbenutzer Benutzer, die physisch mit dem Zähler interagieren, indem sie ein zum TOE gehörendes Display und eine Tastatur verwenden oder über eine separate Komponente, die über eine direkte Schnittstelle mit dem Zähler verbunden ist.

Netzbenutzer Entitäten, die mit dem Zähler über die logischen, kommunikationsbasierten Funktionsschnittstellen interagieren, die der Zähler bietet. Auf diese funktionalen Schnittstellen darf über WAN, Nachbarschaftsnetz oder lokales Netz zugegriffen werden.

Die SFRs in diesem Schutzprofil definieren keine spezifischen Rollen oder privilegierten Vorgänge auf dem Zähler, sondern erfordern die Spezifikation aller derartigen Rollen und privilegierten Vorgänge, die in die Sicherheitsvorgaben aufzunehmen sind.⁵ Eine solche Rolle könnte beispielsweise die eines Servicetechnikers sein, der Installations-, Inbetriebnahme-, Wartungs- oder Diagnosetätigkeiten am Zähler durchführt: Für die Zwecke dieses Schutzprofils werden solche Benutzer je nach den Schnittstellen, die sie für die Interaktion mit dem TOE verwenden, als Direkt- oder Netzbenutzer behandelt. Es ist jedoch auch möglich, dass Servicetechniker Zugang zu privilegierten Funktionen benötigen, und alle derartigen Funktionen sind in die Sicherheitsvorgaben als Teil der Definition der operativen Schnittstellen des TOE aufzunehmen.

Bedrohungsagenten werden als Einzelpersonen (oder Gruppen) betrachtet, die mit dem TOE interagieren und dabei dieselben Schnittstellen und Verfahren verwenden, die auch Direktbenutzern und Netzbenutzern wie oben zur Verfügung stehen.

6.3 Bedrohungen

6.3.1 Allgemeines

Die folgenden Bedrohungen sind für den TOE definiert. Der Angreifer (d. h. der „Bedrohungsagent“), der in jeder der Bedrohungen beschrieben wird, ist ein Subjekt, das für die betreffende Aktion nicht autorisiert ist: Der Angreifer darf sich entweder als ein völlig unbekannter Benutzer oder als eine der legitimen externen Entitäten in diesem Abschnitt ausgeben (in diesem Fall hat der Angreifer jedoch keinen Zugang zu den Authentifizierungs- oder Autorisierungsdaten des Benutzers oder der externen Entität).

6.3.2 T.NetworkDisclosure - Unbefugte Datenoffenlegung durch Netzzugang

Ein Angreifer verschafft sich über eine Netzwerkschnittstelle Zugang zu Daten, die den Schutz der Vertraulichkeit erfordern (dies wird entsprechend den im TOE implementierten Richtlinien definiert, umfasst aber üblicherweise private und geheime Schlüssel, Referenz-Authentifizierungs-/Autorisierungsdaten wie unverschlüsselte Kennwort- oder PIN-Werte und persönliche Daten wie Verbrauchs- und Finanzdaten, die im Zähler gespeichert sind). Der Zugriff könnte entweder durch das Abfangen von Nachrichten auf dem Weg zum oder vom TOE oder durch die Ausführung eines Befehls (ohne Autorisierung) zum Fernzugriff auf im TOE gespeicherte Daten erfolgen.

6.3.3 T.DirectDisclosure - Unbefugte Datenoffenlegung durch Direktzugang

Ein Angreifer verschafft sich Zugang zu Daten, die den Schutz der Vertraulichkeit erfordern (definiert nach den im TOE implementierten Richtlinien, wie für T.NetworkDisclosure beschrieben). Der Zugriff erfolgt

⁵ So werden z. B. die erforderlichen Rollen in FMT_SMR.1 festgelegt und die Regeln für die Autorisierung und Zugriffskontrolle in FDP_ACF.1 und FDP_IFF.1/Msgs. Der ST-Autor darf sich auch dafür entscheiden, die Definition von Externen Entitäten in diesem Abschnitt zu präzisieren, um mehr Klarheit und eine bessere Granularität in den SFRs zu ermöglichen.

möglicherweise entweder durch das Abfangen von Nachrichten, die sich auf dem Weg zum oder vom TOE befinden, oder durch die Ausführung eines Befehls (ohne Autorisierung) über eine direkte Schnittstelle, um auf die im TOE gespeicherten Daten zuzugreifen (wobei zu beachten ist, dass ein direkter Angreifer zusätzlich zu den Netzwerkschnittstellen auch alle anderen Schnittstellen des Zählers, wie z. B. das Display und die Tastatur, nutzen kann). Darüber hinaus könnte der Angreifer versuchen, sich unbefugt physischen Zugang zum Zähler zu verschaffen, indem er auf interne Schnittstellen und Komponenten zugreift (z. B. um direkt auf den Speicher zuzugreifen, ohne die vorgesehenen Schnittstellen zu verwenden).

6.3.4 T.NetworkDataMod - Unbefugte Datenveränderung durch Netzzugang

Ein Angreifer verschafft sich über eine Netzwerkschnittstelle Zugang zu Daten in einer Weise, die eine unbefugte Änderung von Daten ermöglicht, für die eine vorherige Genehmigung zur Änderung erforderlich ist (dies ist nach den im TOE implementierten Richtlinien definiert). Solche Daten können unter anderem Zählerdaten, Konfigurationsdaten (einschließlich der Zählerzeit) oder andere Betriebsparameter umfassen (z. B. ob der Zähler im Kredit- oder Vorauszahlungsmodus arbeitet). Der Zugriff erfolgt unter Umständen durch Ändern, Wiederverwenden oder Fälschen von Nachrichten, die zum oder vom TOE übertragen werden, oder durch Ausführen eines Befehls (ohne Autorisierung) zur Fernänderung von im TOE gespeicherten Daten.

6.3.5 T.DirectDataMod - Unbefugte Datenveränderung durch Direktzugang

Ein Angreifer verschafft sich auf eine Art und Weise Zugang zu Daten, die eine unbefugte Änderung von Daten ermöglicht, für die eine vorherige Genehmigung zur Änderung erforderlich ist (definiert nach den im Zähler implementierten Richtlinien). Der Anwendungsbereich solcher Daten ist wie bei T.NetworkDataMod definiert. Der Zugriff erfolgt möglicherweise durch die Änderung, Wiederverwendung oder Fälschung von Nachrichten, die sich auf dem Weg zum oder vom TOE befinden, oder durch die Ausführung eines Befehls (ohne Autorisierung) über eine direkte Schnittstelle, um die im TOE gespeicherten Daten zu verändern (wobei zu beachten ist, dass ein direkter Angreifer zusätzlich zu den Netzwerkschnittstellen auch alle anderen Schnittstellen des Zählers, wie z. B. das Display und die Tastatur, nutzen kann). Darüber hinaus könnte der Angreifer versuchen, sich unbefugt physischen Zugang zum Zähler zu verschaffen, indem er auf interne Schnittstellen und Komponenten zugreift (z. B. um direkt auf den Speicher zuzugreifen, ohne die vorgesehenen Schnittstellen zu verwenden).

6.3.6 T.Malfunction - Gefährdung von Werten aufgrund einer Fehlfunktion des TOE

Der TOE kann unter Umständen einen Fehler entwickeln, der dazu führt, dass andere Sicherheitseigenschaften geschwächt werden oder ausfallen, wodurch die Energieversorgung deaktiviert wird. Wenn andere Sicherheitseigenschaften geschwächt sind, könnte dies alle Datenbestände betreffen und dazu führen, dass eine der anderen Bedrohungen realisiert wird.

6.4 Organisatorische Sicherheitsrichtlinien

6.4.1 Allgemeines

Der TOE muss die folgenden organisatorischen Sicherheitsrichtlinien einhalten.

6.4.2 P.Logging - Protokollierung von Sicherheitsereignissen

Der TOE muss ein Protokoll der Sicherheitsereignisse führen und das Protokoll gegen unbefugte Änderung schützen.

Anwendungshinweis 1

Dieses Protokoll wird benötigt, um die Fehlerdiagnose, die Bestimmung oder Bestätigung des Zählerzustands und die Untersuchung verdächtiger Ereignisse zu unterstützen.

6.4.3 P.Alarms - Alarmierung bei kritischen Ereignissen

Der TOE muss eine Alarmmeldung an ein definiertes Ziel senden, wenn eines der in einer Liste definierten kritischen Ereignisse eintritt. Der Alarm muss bei oder vor der nächsten Standardkommunikationsmöglichkeit des Zählers gesendet werden.

Anwendungshinweis 2

Die spezifischen Ziele und Ereignisse sind nicht im Schutzprofil angegeben, sondern werden vom ST-Autor definiert.⁶

6.5 Annahmen

6.5.1 A.ExternalData - Schutz von Daten außerhalb der TOE-Steuerung

Wenn Kopien von Daten, die durch den TOE geschützt sind, außerhalb des TOE verwaltet werden, müssen die entsprechenden externen Anwendungen und anderen Entitäten einen angemessenen Schutz für diese Daten bieten.

6.5.2 A.AuditSupport - Überprüfung der Auditdaten

Der vom TOE erzeugte Prüfpfad wird von einer geeigneten externen Prüfstelle nach einem für die AMI festgelegten Prüfverfahren erfasst, gepflegt und überprüft.

Anwendungshinweis 3

Der Prüfpfad besteht aus dem Protokoll der vom TOE aufgezeichneten Sicherheitsereignisse.

6.5.3 A.InspectionSupport - Prüfung der Integrität von Zählern

Jedes einzelne System für die Einführung und den Betrieb einer AMI umfasst Maßnahmen (auf der Grundlage einer Risikoanalyse), um Manipulationen an den Zählern zu verhindern und geeignete Prüfungen der Zählerintegrität zu unterstützen.

Anwendungshinweis 4

Der Begriff „System für die Einführung und den Betrieb einer AMI“ gilt für einzelne AMI mit unterschiedlichen Normen, Architekturdefinitionen sowie Betriebsrichtlinien und -befugnissen. Das System ist der Punkt, an dem Richtlinien für Aktivitäten wie Prüfungen definiert und durchgesetzt werden.

6.5.4 A.UniqueSubjectIDs – Subjekte haben eindeutige Identifikationsschlüssel

Externe Subjekte verwenden bei ihren Interaktionen mit dem TOE eindeutige Identifikationsschlüssel. (Es ist zu beachten, dass diese Anforderung von der Anforderung E im Datenschutz- und Sicherheitskonzept der Koordinationsgruppe für Smart Meter – Teil IV – abgeleitet ist.)

⁶ Die Definition der Ereignisse ist in FAU_ARP.2 erforderlich.

7 Sicherheitszielsetzungen

7.1 Allgemeines

In diesem Abschnitt werden die Sicherheitsziele für den TOE und seine operative Umgebung ermittelt und definiert.

Die Sicherheitszielsetzungen spiegeln die erklärte Absicht wider, wirken den festgestellten Bedrohungen entgegen und stehen im Einklang mit den festgelegten organisatorischen Sicherheitsrichtlinien und -annahmen.

7.2 Sicherheitszielsetzungen für den TOE

7.2.1 Allgemeines

Die folgenden Sicherheitszielsetzungen beschreiben Sicherheitseigenschaften, die vom TOE zu implementieren sind.

7.2.2 O.Authorization – Berechtigung für den Zugriff auf TOE-Daten und -Funktionen

Der TOE muss die Berechtigung jeder direkten oder vernetzten Entität, die Zugang zu seinen Daten und Funktionen beantragt, prüfen und den Zugang auf der Grundlage des Ergebnisses dieser Prüfung gewähren oder verweigern. Der TOE muss auf wiederholte, aufeinanderfolgende, erfolglose Autorisierungsversuche reagieren, indem er vorübergehend alle weiteren Autorisierungsanfragen für eine definierte Zeitspanne ablehnt. Erfolgreiche Autorisierungsversuche verfallen nach einer bestimmten Zeitspanne.

7.2.3 O.Messages – Nachrichtenschutz

Der TOE muss den gesamten Datenaustausch so durchführen, dass die Sicherheit auf dem gesamten Weg zwischen dem TOE und dem Absender/Empfänger der Nachricht sichergestellt ist (wobei der Empfänger der Nachricht der beabsichtigte Endempfänger ist). Der Datenaustausch muss zumindest einen Schutz gegen Wiederverwendung, unbefugte Offenlegung, unbefugte Änderung und Fälschung von authentischen Nachrichten umfassen. Der Schutz muss unabhängig von dem zugrunde liegenden Kommunikationsprotokoll sein.

7.2.4 O.DataAtRest – Schutz gespeicherter Daten

Der TOE muss die gespeicherten Daten gegen unbefugte Offenlegung und Änderung nach einer für die jeweiligen Datenarten festgelegten Richtlinie schützen.

7.2.5 O.Crypto – Zugelassene kryptographische Mechanismen

Der TOE muss Schutzmechanismen unter Verwendung dokumentierter kryptographischer Mechanismen, der Generierung von Zufallsbits und Schlüsselverwaltungstechniken implementieren, die auf anerkannten offenen Normen beruhen.

Anwendungshinweis 5

Die Behörde, die für die Zulassung der kryptographischen Normen zuständig ist, wird durch das/die AMI-System(e) bestimmt, in dem/denen der Zähler verwendet werden soll. Es ist ein wesentlicher Bestandteil dieser Zulassung, dass sie eine Bestätigung der Verwendung geeigneter kryptographischer Parameter (z. B. Algorithmen, Modi, Initialisierungswerte, Schlüssellängen) darstellt.

7.2.6 O.Interfaces – Nicht-operative Schnittstellen deaktiviert

Der TOE muss alle Schnittstellen deaktivieren, die für den normalen Betrieb des Zählers nicht erforderlich sind. Das Verfahren zur Deaktivierung solcher Schnittstellen muss verhindern, dass sie zur Beeinträchtigung der anderen Sicherheitszielsetzungen des TOE verwendet werden können.

7.2.7 O.Resilience – Resilienz gegen Ausfälle

Der TOE muss in einer definierten und sicheren Weise anlaufen und sich von Fehlern erholen.

7.2.8 O.SecureUpdate – Durch digitale Signatur geschützte Updates

Die TOE-Firmware darf nur über eine sichere Updatefunktion aktualisiert werden können, die die Integrität und Authentizität des Updates durch eine digitale Signatur schützt.

Anwendungshinweis 6

Der Begriff „Firmware“ wird in diesem Schutzprofil verwendet, um jede im TOE vorhandene ausführbare Software oder Firmware zu beschreiben. Die sichere Aktualisierungsfunktion gilt für die gesamte Firmware des TOE, die aktualisiert werden kann.

7.2.9 O.Logging – Protokollierung von Sicherheitsereignissen

Der TOE muss ein Protokoll der Sicherheitsereignisse führen und das Protokoll gegen unbefugte Änderung schützen.

7.2.10 O.Alarms – Alarme für kritische Ereignisse

Der TOE muss eine Alarmmeldung an ein definiertes Ziel senden, wenn eines der in einer Liste definierten Ereignisse eintritt. Der Alarm muss bei oder vor der nächsten Standardkommunikationsmöglichkeit des Zählers gesendet werden.

7.3 Sicherheitszielsetzungen für die operative Umgebung

Die folgenden Sicherheitszielsetzungen beziehen sich auf die TOE-Umgebung.

7.3.1 OE.ExternalData – Schutz von Daten außerhalb der TOE-Steuerung

Wenn Kopien von Daten, die durch den TOE geschützt sind, außerhalb des TOE verwaltet werden, müssen die entsprechenden externen Anwendungen und anderen Entitäten einen angemessenen Schutz für diese Daten bieten.

7.3.2 OE.AuditSupport – Überprüfung der Auditdaten

Der vom TOE erzeugte Prüfpfad muss von einer geeigneten externen Prüfstelle nach einem für die AMI festgelegten Prüfverfahren erfasst, gepflegt und überprüft werden.

7.3.3 OE.InspectionSupport – Prüfungen der Integrität von Zählern

Das System für die Einführung und den Betrieb einer AMI muss Maßnahmen (auf der Grundlage einer Risikoanalyse) umfassen, um Manipulationen an den Zählern zu verhindern und geeignete Prüfungen der Zählerintegrität zu unterstützen.

7.3.4 OE.UniqueSubjectIDs – Subjekte haben eindeutige Identifikationsschlüssel

Externe Subjekte müssen bei ihren Interaktionen mit dem TOE eindeutige Identifikationsschlüssel verwenden. (Es ist zu beachten, dass diese Anforderung von der Anforderung E im Datenschutz- und Sicherheitskonzept der Koordinationsgruppe für Smart Meter – Teil IV – abgeleitet ist.)

8 Erweiterte Definitionen der Komponenten

8.1 Allgemeines

In den Common Criteria ist es obligatorisch, die Anforderungen an Komponenten aus CC Teil 2 oder CC Teil 3 zu stellen, wobei es zwei Ausnahmen gibt:

- es gibt Sicherheitszielsetzungen für den TOE, die nicht in Teil 2 SFRs umgewandelt werden können, oder es gibt Anforderungen von Dritten (z. B. Gesetze, Normen), die nicht in Teil 3 SARs umgewandelt werden können (z. B. bezüglich
- Evaluierung der Kryptographie; eine Sicherheitszielsetzung kann umgesetzt werden, aber nur mit großer Schwierigkeit und/oder Komplexität auf der Grundlage von Komponenten in CC Teil 2 und/oder CC Teil

In beiden Fällen ist der PP/ST-Autor verpflichtet, seine eigenen Komponenten zu definieren. Diese definierten Komponenten werden als erweiterte Komponenten bezeichnet. Eine genau definierte erweiterte Komponente ist erforderlich, um den erweiterten SFRs und den auf dieser Komponente basierenden SARs Kontext und Bedeutung zu verleihen.

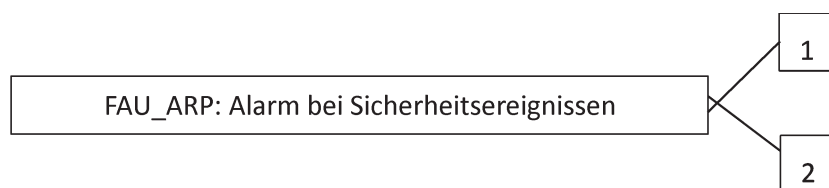
8.2 Alarm bei Sicherheitsereignissen (FAU_ARP.2)

Diese Komponente erweitert die bestehende Familie FAU_ARP und fügt eine andere Art von Alarm hinzu, der im Gegensatz zu FAU_ARP.1 nicht direkt an das Auditprotokoll gebunden ist. Elemente der Definition, die nur für FAU_ARP.1 relevant sind, werden hier nicht wiederholt.

Verhalten der Familie

Diese Familie definiert die Reaktion, die bei erkannten Ereignissen, aus denen sich eine mögliche Sicherheitsverletzung ergibt, zu ergreifen ist.

Nivellierung der Komponenten:



Management: FAU_ARP.2

Standardmäßig sind keine Managementaufgaben definiert.

Audit: FAU_ARP.2

Es gibt keine Aktionen, die standardmäßig als prüfbar definiert sind.

FAU_ARP.2 *Alarm bei Sicherheitsereignissen*

Hierarchisch zu: keine anderen Komponenten

Abhängigkeiten: keine Abhängigkeiten

- | | |
|-------------|---|
| FAU_ARP.2.1 | Die TSF muss bei folgenden Ereignissen eine Alarmmeldung an das angegebene Ziel senden: [Aufgabe: <i>Liste der Ereignisse und Ziel des Alarms für jedes Ereignis</i>]. |
| FAU_ARP.2.2 | Die TSF muss in jeder Alarmmeldung mindestens die folgenden Informationen enthalten:
a) Datum und Uhrzeit des Ereignisses;
b) Art des Ereignisses. |
| FAU_ARP.2.3 | Die TSF muss die folgenden zusätzlichen Alarminformationen enthalten: [Aufgabe: <i>Liste der Alarmmeldungen und der zugehörigen Zusatzinformationen</i>]. |
| FAU_ARP.2.4 | Die TSF muss Alarme nach den folgenden Zeitregeln senden: [Aufgabe: Regeln, die festlegen, wann ein Alarm in Bezug auf die Erkennung des Ereignisses gesendet werden muss]. |

8.3 Vertrauenswürdiges Software-Update (FPT_TSU.1)

Die Zähler-Firmware muss durch ein Aktualisierungsverfahren mit digital signierten Updates, die authentifiziert werden können und deren Integrität zwischen dem Urheber und dem Zähler gesichert ist, vor Manipulationen geschützt werden. Ein Zähler, der mit diesem PP konform ist, lässt keine Aktualisierung der TOE-Firmware zu, die nicht über den sicheren Aktualisierungsprozess erfolgt.

Verhalten der Familie

Die Komponenten dieser Familie erfüllen die Anforderungen an eine vertrauenswürdige Software/Firmware-Aktualisierung der TSF.

Nivellierung der Komponenten:



Management: FPT_TSU.1

Standardmäßig sind keine Managementaufgaben definiert.

Audit: FPT_TSU.1

Es gibt keine Aktionen, die standardmäßig als prüfbar definiert sind.

FPT_TSU.1 *Vertrauenswürdiges Software-/Firmware-Update*

Hierarchisch zu: keine anderen Komponenten

Abhängigkeiten: FCS_COP.1

- | | |
|-------------|---|
| FPT_TSU.1.1 | Die TSF muss [Aufgabe: Liste der autorisierten Rollen] die Möglichkeit bieten, [Auswahl, eine von: die aktuell ausgeführte Version der TOE-Software/Firmware, die |
|-------------|---|

aktuell ausgeführte und die zuletzt heruntergeladenen Versionen der TOE-Software/Firmware] abzufragen.

- FPT_TSU.1.2 Die TSF muss Mittel zur Authentifizierung und Verifizierung der Integrität von Software-/Firmware-Aktualisierungen für den TOE vor der Installation dieser Aktualisierungen unter Verwendung eines digitalen Signaturmechanismus bereitstellen, der die folgenden Anforderungen erfüllt: [Aufgabe: *Mechanismusspezifikation*].
- FPT_TSU.1.3 Die TSF muss Mittel bereitstellen, um die folgenden zusätzlichen Eigenschaften von Software-/Firmware-Aktualisierungen des TOE vor der Installation dieser Aktualisierungen zu verifizieren: [Aufgabe: *Liste der zusätzlichen Eigenschaften*].
- FPT_TSU.1.4 Die TSF muss [Aufgabe: *Liste der autorisierten Rollen*] die Möglichkeit bieten, Aktualisierungen der TOE-Software/Firmware zu aktivieren.

Anwendungshinweis 7

In FPT_TSU.1.1 ist die aktuell ausgeführte Version möglicherweise nicht mit der zuletzt heruntergeladenen Version identisch, da eine heruntergeladene Version noch nicht zwangsläufig aktiviert worden sein muss.

Die kryptographischen Vorgänge, die zur Umsetzung des Mechanismus der digitalen Signatur in FPT_TSU.1.2 verwendet werden, müssen in Iterationen von FCS_COP.1 angegeben werden.

Beispiele für die in FPT_TSU.1.3 festgelegten Eigenschaften sind die Sicherstellung, dass die Aktualisierung für den TOE-Typ oder die Instanz bestimmt ist, oder die Sicherstellung, dass es sich bei der Aktualisierung um eine neuere Version als die aktuell ausgeführte Version handelt.

Die Aktivierung in FPT_TSU.1.4 führt dazu, dass die aktualisierte *Software/Firmware* ausgeführt wird.

Wenn der TOE die Abfrage der aktuell ausgeführten Version nicht unterstützt, ist es legitim, die Aufgabe der Liste der Rollen in FPT_TSU.1.1 mit „Keine“ abzuschließen, und in diesem Fall wird das SFR-Element als trivial erfüllt behandelt.

8.4 Grundlegende TSF-Selbstprüfung (FPT_BST.1)

Die hier definierte erweiterte Komponente ist eine vereinfachte Version von FPT_TST.1 in Übereinstimmung mit ISO/IEC 15408-2.

Verhalten der Familie

Die Komponenten dieser Familie erfüllen die Anforderungen für die Selbstprüfung der TSF zu bestimmten Zeiten auf korrekten Betrieb.

Nivellierung der Komponenten:



Management: FPT_BST.1

Standardmäßig sind keine Managementaufgaben definiert.

Audit: FPT_BST.1

Die folgenden Aktionen sollten auditierbar sein, wenn die Generierung von FAU_GEN-Sicherheitsauditdaten in der PP/ST enthalten ist:

- Anzeige, dass die TSF-Selbstprüfung abgeschlossen wurde.

FPT_BST.1 *Grundlegende TSF-Selbstprüfung*

Hierarchisch zu: keine anderen Komponenten

Abhängigkeiten: keine Abhängigkeiten

FPT_BST.1.1 Die TSF muss eine Reihe der folgenden Selbstprüfungen durchführen [Auswahl: bei der ersten Inbetriebnahme (beim Einschalten), in regelmäßigen Abständen während des normalen Betriebs, auf Verlangen des autorisierten Benutzers, unter den Bedingungen [Aufgabe: Bedingungen, unter denen Selbstprüfungen durchgeführt werden sollten]], um den korrekten Betrieb der TSF nachzuweisen: [Aufgabe: Liste der von der TSF durchgeführten Selbstprüfungen].

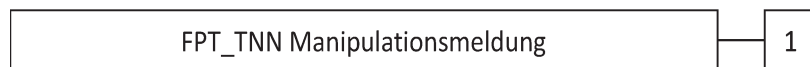
8.5 Manipulationsmeldung (FPT_TNN.1)

Die hier definierte erweiterte Komponente weist einige Ähnlichkeiten mit FPT_PHP.2 in Übereinstimmung mit ISO/IEC 15408-2 auf, enthält jedoch eine Anforderung zur aktiven Manipulationserkennung, die für Geräte wie Smart Meter besser geeignet ist.

Verhalten der Familie

Die Komponenten dieser Familie befassen sich mit den Anforderungen für die Meldung von definierten Manipulationsszenarien an bestimmten Elementen des TOE. Dies unterscheidet sich von FPT_PHP.1 und FPT_PHP.2 durch die Definition spezifischer Manipulationsszenarien und die Möglichkeit der Meldung über eine bestimmte Schnittstelle und nicht an einen bestimmten Benutzer oder eine bestimmte Rolle.

Nivellierung der Komponenten:



Management: FPT_TNN.1

Standardmäßig sind keine Managementaufgaben definiert.

Audit: FPT_TNN.1

Die folgenden Aktionen sollten auditierbar sein, wenn die Generierung von FAU_GEN Sicherheitsauditdaten in der PP/ST enthalten ist:

- erkannte Manipulationsereignisse.

FPT_TNN.1 *Manipulationsmeldung*

Hierarchisch zu: keine anderen Komponenten

Abhängigkeiten: keine

FPT_TNN.1.1 Die TSF muss [Aufgabe: *Liste der TSF-Geräte/Elemente, für die eine aktive Erkennung erforderlich ist*] überwachen und [Aufgabe: *benannte(n) Benutzer, Rolle(n) oder Schnittstelle(n)*] benachrichtigen, wenn physische Manipulationen der folgenden Arten stattgefunden haben: [Aufgabe: *Liste der physischen Manipulationsszenarien*].

Anwendungshinweis 8

Die zweite Aufgabe („benannter Benutzer, Rolle oder Schnittstelle“) beschreibt die Art und Weise, wie die Meldung übermittelt wird: durch Kommunikation mit einer bestimmten Person oder durch Verwendung einer bestimmten Schnittstelle (oder beides). Die Verwendung einer Schnittstelle könnte z. B. ein Licht auf einem Gerätepanel, das Senden einer bestimmten Alarmmeldung oder die Aufzeichnung eines bestimmten Protokolleintrags umfassen. Im Falle eines Protokolleintrags sollte der Inhalt des Protokolleintrags unter Verwendung eines geeigneten FAU-SFR beschrieben werden, und der Schutz des Protokolls gegen Veränderung (vgl. FAU_STG.1) im Zusammenhang mit dem Manipulationsereignis sollte in der Kurzbeschreibung des TOE beschrieben werden.

8.6 Generierung von Zufallszahlen (FCS_RNG.1)

8.6.1 Verhalten der Familie

Diese Familie legt Qualitätsanforderungen für die Generierung von Zufallszahlen fest, die für kryptographische Zwecke verwendet werden sollen.

Nivellierung der Komponenten:



Management: FCS_RNG.1

Es sind keine Managementaufgaben vorhanden.

Audit: FCS_RNG.1

Es gibt keine Aktionen, die als prüfbar definiert sind.

FCS_RNG.1 *Generierung von Zufallszahlen*

Hierarchisch zu: keine anderen Komponenten

Abhängigkeiten: keine Abhängigkeiten

FCS_RNG.1.1 Die TSF muss einen [Auswahl: physikalisch, nicht-physikalisch echt, deterministisch, hybrid-physikalisch, hybrid-deterministisch] Zufallszahlengenerator bereitstellen, der Folgendes implementiert: [Aufgabe: *Liste der Sicherheitsfähigkeiten*].

FCS_RNG.1.2 Die TSF muss [Auswahl: Bits, Oktette von Bits, Zahlen [Aufgabe: *Format der Zahlen*]] bereitstellen, die [Aufgabe: *eine definierte Qualitätskennzahl*] erfüllen.