TECHNISCHE SPEZIFIKATION

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

CEN/CLC/TS 17880

Dezember 2022

ICS 33.200; 35.030; 35.240.99

Deutsche Fassung

Schutzprofil für Smart Meter - Mindestsicherheitsanforderungen

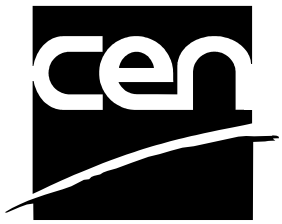
Protection Profile for Smart Meter - Minimum Security requirements

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 des CEN 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- und CENELEC-Mitglieder sind die nationalen Normungsinstitute und elektrotechnischen Komitees 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 Centre:
Rue de la Science 23, B-1040 Brussels

Inhalt

Seite

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 EAL.3+ 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)