TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/CLC/TS 17880

December 2022

ICS 33.200; 35.030; 35.240.99

English version

Protection Profile for Smart Meter - Minimum Security requirements

Schutzprofil für Smart Meter - Mindestsicherheitsanforderungen

This Technical Specification (CEN/TS) was approved by CEN on 4 December 2022 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN and CENELEC will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN and CENELEC members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

CEN/CLC/TS 17880:2022 - Preview only Copy via ILNAS e-Shop

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

© 2022 CEN/CENELEC All rights of exploitation in any form and by any means reserved worldwide for CEN national Members and for CENELEC Members.

Ref. No. CEN/CLC/TS 17880:2022 E

Contents

Page

CEN/CLC/TS 17880:2022 - Preview only Copy via ILNAS e-Shop

European foreword

This document (CEN/CLC/TS 17880:2022) has been prepared by Technical Committee CEN/CLC JTC 13 “cybersecurity and data protection”, the secretariat of which is held by DIN.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

It is based on the “Protection Profile for Smart Meter Minimum Security requirements” Version 1.0, 30 October 2019 (CENCLCETSI_SMCG/Sec/00156/DC) created by the CEN/CENELEC/ETSI Coordination Group on Smart Meters (CG-SM).

Any feedback and questions on this document should be directed to the users’ national standards body. A complete listing of these bodies can be found on the CEN website.

According to the CEN/CENELEC Internal Regulations, the national standards organisations of the following countries are bound to announce this Technical Specification: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

CEN/CLC/TS 17880:2022 - Preview only Copy via ILNAS e-Shop

Introduction

This Protection Profile describes a set of security requirements for smart meters, based on the 'minimum security requirements' for components of Advanced Metering Infrastructures. The requirements in Smart Meter Co-ordination Group Privacy and Security Approach –Part IV are based on the concept that there are a common/generic set of underlying 'minimum' security requirements associated with smart metering requirement specifications in a number of EU Member States. Members of the ad hoc CG-SM Task Force on Privacy and Security as a result developed a set of generic minimum requirements that are valid for most of the European Member States. From this set, the requirements applicable to smart meters (as opposed to other parts of the AMI) have then been used as the basis for this Protection Profile by translating them, with specification of additional detail where necessary, into Common Criteria Security Functional Requirements (SFRs) and refinements to the Security Assurance Requirements (SARs)[1]. The requirements defined in this Protection Profile can therefore serve as a basis for specific requirements of individual EU Member States, based on a risk analysis that has assessed the specific assets and actors applicable to their scheme.

The aim of this Protection Profile is to come to an European approach for the security certification of Smart Meters. The Cyber Security Act of the European Commission, that came into act in June 2019, asks for the development of European certification schemes for products, processes, and services in order to prevent fragmentation of the market by various national certification schemes. The SM-CG Working Group on Privacy and Security is of the opinion that Common Criteria provide a cost effective and efficient method for an agreement between manufacturers, customers and security evaluators as to what assurance level a product shall be provided based upon a protection profile and a security target for Smart Meters.

The Task Force recognizes that some national schemes already exist and have proven their value, such as the French CSPN (Certification Sécurité de Premier Niveau) approach and also the CPA (Commercial Product Assurance) approach in Great Britain and is of the opinion that it must be possible for these national approaches to be continued. In parallel the Task Force believes that an approach based on Common Criteria EAL.3+ and the already existing mutual recognition of CC certificates among 17 European countries, is a valuable alternative for European countries that do not have an existing certification scheme for Smart Meters yet.

The content of a Protection Profile is defined in ISO/IEC 15408-1.

Clauses 4 to 7 based on general concepts – they are therefore intended to be read by general readers. Other sections specify more detailed requirements and require some familiarity with Common Criteria concepts in ISO/IEC 15408 (all parts). These more detailed requirements are used by Common Criteria experts within developer organisations when to write a Security Target (ST) that claims conformance to this Protection Profile for their product and identifies the product-specific ways in which the requirements are met and implemented in the product. During the evaluation of the product, the evaluators will check the conformance of the developer's ST to this Protection Profile, as well as the conformance of the product to the requirements in the ST.

Any security functionality on the meter is an additional functionality and this does not have any influence on the metrological characteristics of the meter.

[1] In general, the refinements to Security Assurance Requirements are made in order to make a clearer definition of the evaluation activities required, and to improve the consistency of evaluations against the requirements in this Protection Profile.

CEN/CLC/TS 17880:2022 - Preview only Copy via ILNAS e-Shop

1 Scope

This document specifies a security certification approach for smart electricity meters. It provides a general solution for security certification to avoid fragmentation and to enable mutual recognition of certificates in Europe. It defines the functional requirements and assurance criteria (see the Common Criteria in ISO/IEC 15408 (all parts)) for security certification.

This Protection Profile does not define specific types of sensitive personal information or personally identifiable information.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at https://www.electropedia.org/
- ISO Online browsing platform: available at https://www.iso.org/obp

3.1
administrator
role that has a level of trust with respect to all policies implemented by the TSF in a generic term for a privileged role that has access to sensitive operations affecting the configuration and operation of the meter

3.2
advanced metering infrastructure
infrastructure which allows two way communications between the Head-End System and the meter(s)

Note to entry: An Advanced Metering Infrastructure can also be linked to other in house devices

3.3
assurance
grounds for confidence that a TOE meets the SFRs

3.4
consumer
end user of the metered quantity (electricity, gas, water or thermal energy)

CEN/CLC/TS 17880:2022 - Preview only Copy via ILNAS e-Shop

3.5
critical event
event that can take place in a smart meter and that is particularly significant for supply or security of the meter

Note 1 to entry: The critical events for a meter conformant with this Protection Profile are defined as part of FAU_ARP.2 in section 9.3.6.1)

3.6
digital signature
cryptographic techniques applied to data in order to allow verification of its integrity and authenticity

3.7
direct interface
interface to the meter that does not involve access from external networks

Note to entry 1: External networks can be WAN, Neighbourhood Network or Local Network

3.8
electromagnetic
EM
physical property related to the interrelation of electric currents or fields and magnetic fields

3.9
evaluator
person or group that carries out a security evaluation of the TOE

Note 1 to entry: An example of an evaluation standard is ISO/IEC 15408-3 with the associated evaluation methodology given in ISO/IEC 18045.

3.10
firmware
executable code of a meter that is stored in hardware

Note to entry 1: For the purposes of this Protection Profile the relevant up-date process is defined in FPT_TSU.1, see section 9.3.4.6

3.11
hand-held terminal unit
portable device for reading and programming equipment or meters at the consumer's premises or at the access point

CEN/CLC/TS 17880:2022 - Preview only Copy via ILNAS e-Shop

3.12
joint test action group
JTAG
commonly used to refer to the interface defined in IEEE 1149.1 Standard Test Access Port and Boundary-Scan Architecture

3.13
local network
data communication network providing access to local (in-house/building) devices and / or other local networks

3.14
message authentication code
MAC
cryptographic checksum on message data, used to provide assurance that the sender of a message is who they claim to be and that the message is in the form originally sent (subject to the assumption that a cryptographic key is known only to the sender and the receiver)

3.15
message
application-level communication sent to or left for a recipient

Note 1 to entry: The minimum requirements in Smart Meter Co-ordination Group Privacy and Security Approach – Part IV, v1.1, 17 July 2016, that are the source for this Protection Profile require that security is implemented at the application level, independent of protections that might be provided by the communication protocol.

3.16
meter data
meter readings that allow calculation of the quantity of electricity, gas, water, or thermal energy consumed over a period

Note 1 to entry: Meter data thus may include daily and monthly meter readings, interval readings and actual meter register values. Other readings and data may also be included (such as quality data, events and alarms)

3.17
metrology
non TSF part of the TOE that converts a physical property in a digital signal. These functions are governed by the requirements of the Measuring Instruments Directive 2004/22/EC (MID)

3.18
neighbourhood network
data communication network providing access to several premises and / or other neighbourhood networks

3.19
operational interfaces
interfaces required for normal operation of the meter (all other accessible interfaces are disabled)

CEN/CLC/TS 17880:2022 - Preview only Copy via ILNAS e-Shop