



BSI Standards Publication

Protection Profile for Smart Meter — Minimum Security requirements

National foreword

This Published Document is the UK implementation of CEN/CLC/TS 17880:2022.

The UK participation in its preparation was entrusted to Technical Committee IST/33/5, Identity Management and Privacy Technologies.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2023
Published by BSI Standards Limited 2023

ISBN 978 0 539 21312 6

ICS 33.200; 35.030; 35.240.99

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 March 2023.

Amendments/corrigenda issued since publication

Date	Text affected

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

Contents	Page
European foreword	3
Introduction	4
1 Scope.....	5
2 Normative references.....	5
3 Terms and definitions.....	5
4 Target of Evaluation.....	9
5 Conformance Claims	11
6 Security Problem Definition	11
7 Security Objectives.....	15
8 Extended Components Definitions	16
9 Security Requirements	21
10 Rationales	53
Annex A (informative) Mapping to Minimum Security Requirements	62
Bibliography	72

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.

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 EAL3+ 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.

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)

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

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)

3.20

protection profile

PP

implementation-independent statement of security needs for a TOE type

[Source ISO/IEC 15408-1:2009(en), 3.1.52]

3.21

role

entitlement of a party to execute a set of one or more commands associated with the role name

3.22

security assurance requirement

SAR

Description of how the TOE is to be evaluated, using the standardised language

3.23

security functional requirement

SFR

translation of the security objectives for the TOE into a set of standardised functional requirements

Note to entry 1: The SFR for the PP are drawn from ISO/IEC 15408-2 (or as extended components defined in section 8)

3.24

sensor

device that translates a physical property in an electric signal

Note to entry 1: a sensor can be a non TSF part of the TOE, or mounted externally

EXAMPLE: a current transformer or a temperature sensor on a water return pipe

3.25

service technician

users who carry out any local installation, commissioning, maintenance or diagnostic activities on a meter

Note to entry 1: these activities may be carried out over direct or network interfaces and service technicians may need access to privileged functions

3.26

smart meters co-ordination group

SM-CG

joint advisory body, combining expertise and resources from the European Standardization Organizations (CEN, CENELEC and ETSI), that provides a focal point concerning smart metering standardisation issues

3.27

security target

ST

implementation-dependent statement of security needs for a specific identified TOE

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

3.28**target of evaluation****TOE**

set of software, firmware, hardware, or a combination of all three, possibly accompanied by guidance

[SOURCE: ISO/IEC 15408-1:2009, 3.1.70, modified]

3.29**TOE security functionality****TSF**

combined functionality of all hardware, software, and firmware of a TOE (3.3.4) that must be relied upon for the correct enforcement of the SFRs (3.3.7)

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

3.30**TSF Data**

data for the operation of the TOE upon which the enforcement of the SFR relies

[Source ISO/IEC 15408-1:2009(en), 3.1.81]

3.31**user****external entity**

human or IT entity interacting with the TOE from outside of the TOE boundary

3.32**wide area network****WAN**

extended data communication network connecting a large number of communication devices over a large geographical area

4 Target of Evaluation

The Target of Evaluation (TOE) is a smart supply meter that monitors, and possibly limits, the consumption of electricity, gas, thermal energy, or water² provided by utilities supply markets and communicates with users via both local ("direct") and network interfaces. The generic architecture of the TOE is shown in Figure 1. (Interfaces are also labelled 'C', 'G1', 'H1' and 'M' to show correspondence with CEN/CLC/ETSI TR 50571)

² Exhaustive list which matches the main media types in the OBIS identification system.

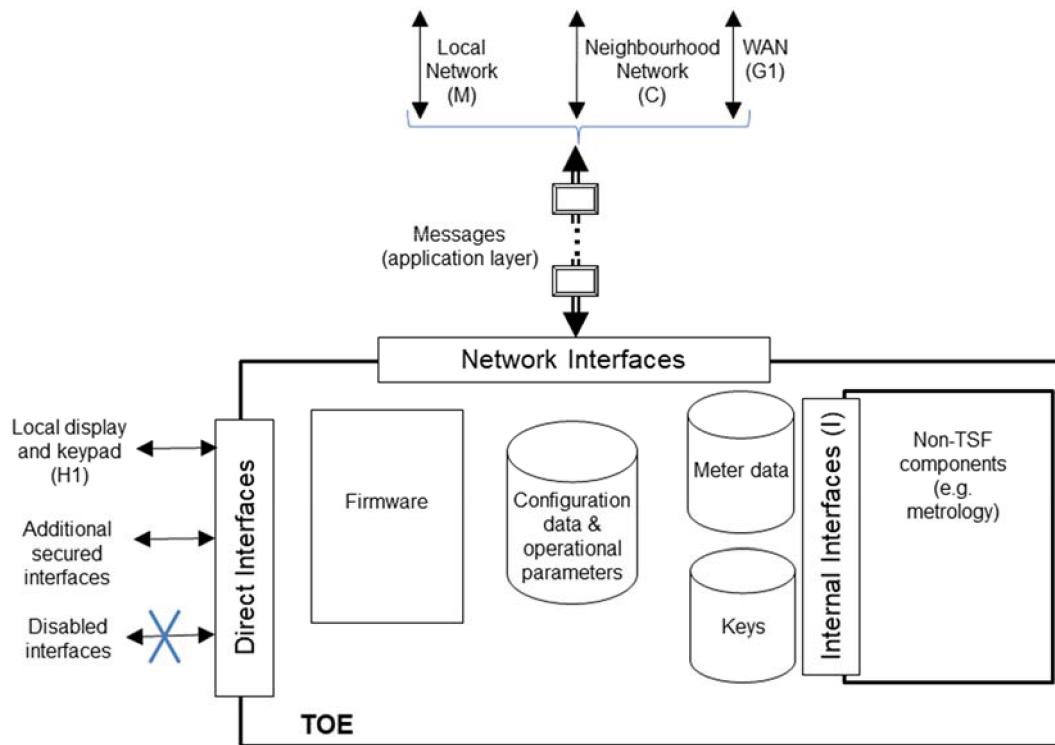


Figure 1 — Generic Smart Meter TOE Architecture

The TOE provides a combination of the following meter-related functions from the reference architecture in [1]:

- List item metrology functions including the conventional meter display (register or index) that are under legal metrological control. When under metrological control, these functions are governed by the requirements of the Measuring Instruments Directive 2004/22/EC (MID)
- additional functions not covered by the MID, typically including features such as remote reading of the meter, advanced tariff and payment systems, and remote enablement and disablement of supply.
- meter communication functions, including network interfaces and direct interfaces.

All smart meters conformant with this PP will implement metrology functions, some additional functions, and communication functions. However, not all meters will implement the same additional functions, nor will they necessarily support all communication interfaces. This PP deals with the unknowns in this regard by requiring identification of the TOE-specific details in an ST conformant to this PP, and by defining refinements of certain SARs to support consistency checks for meter-specific details.

The meter's basic security task is to ensure the integrity of its content, the authenticity and integrity of instructions that it acts on, the confidentiality of data used to provide these other security information and personally identifiable information. Much of this task is therefore concerned with the policies applies by the meter to communications over its various interfaces.

The meter has a backup power source to keep the time during power interruptions.

For the purposes of this PP, all network interfaces are treated simply as exchanging messages of various types with the TOE. Although different interfaces could be using distinct transport and application protocols, this PP requires that all network interfaces are subject to message-level permission controls (i.e. where the permission to act on the content of a message is based on the message itself and possibly contextual factors such as an authenticated end-to-end logical channel used to deliver the messages).

The direct interfaces may include a display and keypad for interaction with the user, and other communication interfaces in accordance with CEN/CLC/ETSI TR 50571. These direct interfaces might be used for communication with other in-home devices, for example to display and analyse consumption data, to communicate with other meters, or to communicate with engineering and maintenance tools such as a hand-held terminal unit.

A meter may have a number of interfaces that have been disabled by the time that it is put into operational use (e.g. interfaces for initialisation, installation, or debugging). These interfaces can have a physical presence on the meter (such as an optical port or debug interface) or can be purely logical interfaces (such as engineering or maintenance functions using the display and keypad). This PP requires that the effective disabling of these interfaces is evaluated in order to confirm that they do not provide methods to bypass the security rules applicable over other interfaces during operational use.

The meter firmware is protected from tampering by a firmware integrity test, and by a secure update method using digitally signed updates that can be authenticated and that have their integrity protected between the originator and the meter. A meter conformant with this PP does not allow update of any TOE firmware other than by using the secure update process.

5 Conformance Claims

This Protection Profile (PP) complies with *ISO/IEC 15408 (all parts)*, for both the content and presentation requirements.

All functional and assurance security requirements laid out in this PP comply with ISO/IEC 15408 Part 2 and ISO/IEC 15408 Part 3 respectively of the aforementioned Common Criteria version.

This PP does not claim conformance to any other PP. The assurance requirement of this Protection Profile is EAL3 augmented with ALC_FLR.3. This Protection Profile requires strict conformance of any Security Target or Protection Profile that claims conformance to this Protection Profile.

6 Security Problem Definition

6.1 Assets

The assets that need to be protected by the TOE are various forms of data, including meter data, configuration data or other operating parameters. Almost all the anticipated benefits to an attacker take the form of accessing one or more of these forms of data – e.g. an attacker might benefit from changing available credit, changing consumption data stored or sent by the TOE, or obtaining a key that enables access to such data. The types of data are not separately defined because in general all data are accessed via one of the direct or network interfaces to the meter, and therefore the focus for the threats is simply on unauthorised access to any of the available data³.

Such definition is done as a part of the description of a specific scheme for operating a metering system of which the smart meter forms a part, and/or in terms of the specific data held and processed by a particular meter type. Cryptographic keys and public key certificates are an example of data which is not specifically identified in this PP: no particular cryptographic scheme or mechanisms are assumed. However, the Security Target for a particular product is required to identify the relevant parameters via its rules for controlling access to configuration of operational parameters, and its rules for ensuring message security and access control. For the purposes of this Protection Profile, the rules for preserving

³ Different types of meters may adopt specific policies that differentiate different types of data, in which case this must be visible in Security Targets by the completion of rules in FDP_ACF.1 and FDP_IFF.1/Msgs.

confidentiality, integrity and authenticity of such information are to be included in the specific authorization, access control and data destruction rules defined in a Security Target⁴.

The other potential goal of an attacker is to be able to remotely disable supply of the energy that the meter controls. This might be achieved by unauthorised access to data as above (e.g. by modifying the balance of a prepayment meter to a level at which the meter disables the supply, or by sending a command that changes an 'enable/disable supply' operating state). Remotely disabling a meter might alternatively be achieved by causing an irrecoverable fault in the meter, and therefore the correct operation of the meter is also treated as an asset in this Protection Profile.

6.2 Entities and Threat Agents

The external entities that interact with the TOE are as follows:

Direct Users users who interact physically with the meter, using a display and keyboard included as part of the TOE, or via a separate component connected to the meter by a direct interface.

Network Users entities who interact with the meter over the logical, communications-based functional interfaces presented by the meter. These functional interfaces may be accessed via WAN, Neighbourhood Network or Local Network.

The SFRs in this Protection Profile do not define specific roles or privileged operations on the meter but require the specification of all such roles and privileged operations to be included in the Security Target⁵. As an example, one such role might be that of a service technician who carries out any installation, commissioning, maintenance, or diagnostic activities on the meter: for the purposes of this Protection Profile such users are treated as direct or network users depending on the interfaces that they use to interact with the TOE. However, it is also possible that service technicians may need access to privileged functions, and any such functions are to be included in the Security Target as part of the definition of the operational interfaces of the TOE.

Threat agents are considered to be individuals (or groups) interacting with the TOE using the same interfaces and methods available to Direct Users and Network Users as above.

6.3 Threats

6.3.1 General

The following threats are defined for the TOE. The attacker (i.e. the 'threat agent') described in each of the threats is a subject who is not authorized for the relevant action: the attacker may present themselves as either a completely unknown user, or as one of the legitimate external entities in section (but in this case the attacker will not have access to the authentication or authorization data for the user or remote entity).

6.3.2 T.NetworkDisclosure - Unauthorised data disclosure via network access

An attacker gains access via a network interface to data that requires protection of confidentiality (this is defined according to the policies implemented in the TOE, but typically includes private and secret keys, reference authentication/authorization data such as unencrypted password or PIN values, and personal data such as consumption and financial data held on the meter). Access might be gained either from intercepting messages in transit to or from the TOE, or by executing a command (without authorization) to remotely access data stored in the TOE.

⁴ Access control rules are described in FDP_ACF.1, authorisation rules in FDP_IFF.1/Msgs, and data subject to specific secure destruction in FDP_RIP.1.

⁵ E.g. roles are specified as required in FMT_SMR.1, and rules defining authorisation and access controls are specified in FDP_ACF.1 and FDP_IFF.1/Msgs. The ST author may also choose to *refine* the definition of External Entities in this section in order to allow greater clarity and better granularity in the SFRs.

6.3.3 T.DirectDisclosure - Unauthorised data disclosure via direct access

An attacker gains access to data that requires protection of confidentiality (defined according to the policies implemented in the TOE, as described for T.NetworkDisclosure). Access might be gained either from intercepting messages in transit to or from the TOE, or by executing a command (without authorization) via a direct interface to access data stored in the TOE (noting that, in addition to any network interfaces a direct attacker will also be able to use any other interfaces present on the meter, such as the display and keypad). In addition, the attacker might attempt unauthorised physical access to the meter by accessing internal interfaces and components (e.g. to access memory directly, without using the intended interfaces).

6.3.4 T.NetworkDataMod - Unauthorised data modification via network access

An attacker gains access via a network interface to data in a way that enables unauthorised modification of data that is intended to require prior authorization for modification (this is defined according to the policies implemented in the TOE). Such data might include meter data, configuration data (including the meter time) or other operating parameters (e.g. such as whether the meter is operating in credit or prepayment mode). Access might be gained from modifying, replaying or forging messages in transit to or from the TOE, or by executing a command (without authorization) to remotely modify data stored in the TOE.

6.3.5 T.DirectDataMod - Unauthorised data modification via direct access

An attacker gains access to data in a way that enables unauthorised modification of data that is intended to require prior authorization for modification (defined according to the policies implemented in the meter). The scope of such data are defined as for T.NetworkDataMod. Access might be gained from modifying, replaying or forging messages in transit to or from the TOE, or by executing a command (without authorization) via a direct interface to modify data stored in the TOE (noting that, in addition to any network interfaces a direct attacker will also be able to use any other interfaces present on the meter, such as the display and keypad). In addition, the attacker might attempt unauthorised physical access to the meter by accessing internal interfaces and components (e.g. to access memory directly, without using the intended interfaces).

6.3.6 T.Malfunction - Asset compromise due to TOE malfunction

The TOE may develop a fault that causes some other security property to be weakened or to fail causing the energy supply to be disabled. Where other security properties are weakened, this could affect any of the data assets and could result in any of the other threats being realized.

6.4 Organisational Security Policies

6.4.1 General

The TOE shall comply with the following organisational security policies.

6.4.2 P.Logging - Logging security events

The TOE shall maintain a log of security events and shall protect the log against unauthorised modification.

Application Note 1

This log is required to assist in diagnosis of faults, determination or confirmation of the meter state, and investigation of suspicious events.

6.4.3 P.Alarms - Alarms sent for critical events

The TOE shall send an alarm message to a defined destination when any of a defined list of critical events occur. The alarm shall be sent at or before the meter's next default communication opportunity.

Application Note 2

The specific destinations and events are not specified in the Protection Profile but are defined by the ST author ⁶.

6.5 Assumptions

6.5.1 A.ExternalData - Protection of data outside TOE control

Where copies of data protected by the TOE are managed outside of the TOE, the relevant external applications and other entities must provide appropriate protection for that data.

6.5.2 A.AuditSupport - Audit data review

The audit trail generated by the TOE will be collected, maintained, and reviewed by an appropriate external audit role according to a defined audit procedure for the AMI.

Application Note 3

The audit trail consists of the log of security events recorded by the TOE.

6.5.3 A.InspectionSupport - Meter integrity inspections

Each particular scheme for deployment and operation of an AMI will include measures (based on risk-analysis) to deter tampering with the meter and to support appropriate inspections of meter integrity.

Application Note 4

The term "scheme for deployment and operation of an AMI" applies to individual AMIs with distinct sets of standards, architecture definitions, and operational policies and authorities. The scheme is the point at which policies for activities such as inspections will be defined and enforced.

6.5.4 A.UniqueSubjectIDs - Subjects have unique identifiers

External subjects will use unique identifiers in their interactions with the TOE. (Note that this requirement is derived from requirement E in Smart Meter Co-ordination Group Privacy and Security Approach –Part IV.

⁶ The definition of the events is required in FAU_ARP.2.

7 Security Objectives

7.1 General

This section identifies and defines the security objectives for the TOE and its operational environment.

Security objectives reflect the stated intent and counter the identified threats, as well as comply with the identified organisational security policies and assumptions.

7.2 Security Objectives for the TOE

7.2.1 General

The following security objectives describe security properties to be implemented by the TOE.

7.2.2 O.Authorization - Authorization for access to TOE data and functions

The TOE shall check the authorization of any direct or network entity requesting access to its data and functions and shall grant or deny access based on the result of that check. The TOE shall respond to repeated, consecutive, unsuccessful authorization attempts by temporarily denying all further authorization requests for a defined period of time. Successful authorization attempts shall expire after a defined period of time.

7.2.3 O.Messages - Message protection

The TOE shall conduct all data exchanges in manner that provides security over the entire path between the TOE and the message originator/recipient (where the message recipient is the intended final receiver). The data exchange shall include protection against at least replay, unauthorised disclosure, unauthorised modification, and forgery of authentic messages. The protection shall be independent of the underlying communication protocol.

7.2.4 O.DataAtRest - Stored data protection

The TOE shall protect stored data against unauthorised disclosure and modification according to a defined policy for the types of data.

7.2.5 O.Crypto - Approved cryptographic mechanisms

The TOE shall implement protection mechanisms using documented cryptographic mechanisms, random bit generation, and key management techniques, based on approved open standards.

Application Note 5

The authority for approval of the cryptographic standards is determined by the AMI scheme(s) in which the meter is intended to be used. It is intrinsic to this approval that it represents confirmation of the use of appropriate cryptographic parameters (e.g. algorithms, modes, initialisation values, key lengths).

7.2.6 O.Interfaces - Non-operational interfaces disabled

The TOE shall disable any interfaces that are not required for normal operation of the meter. The method of disabling such interfaces shall prevent them from being used to compromise the other TOE security objectives.

7.2.7 O.Resilience - Resilience against failures

The TOE shall start-up and recover from failures in a defined and secure way.

7.2.8 O.SecureUpdate - Updates protected using digital signature

The TOE firmware shall be updatable only via a secure update function, using digital signature to protect the integrity and authenticity of the update.

Application Note 6

The term “firmware” is used in this protection profile to describe any executable software or firmware present in the TOE. The secure update function applies to all firmware in the TOE that can be updated.

7.2.9 O.Logging - Security event logging

The TOE shall maintain a log of security events and shall protect the log against unauthorised modification.

7.2.10 O.Alarms - Alarms for critical events

The TOE shall send an alarm message to a defined destination when any of a defined list of events occur. The alarm shall be sent at or before the meter’s next default communication opportunity.

7.3 Security Objectives for the Operational Environment

The following security objectives relate to the TOE environment.

7.3.1 OE.ExternalData - Protection of data outside TOE control

Where copies of data protected by the TOE are managed outside of the TOE, the relevant external applications and other entities shall provide appropriate protection for that data.

7.3.2 OE.AuditSupport - Audit data review

The audit trail generated by the TOE shall be collected, maintained, and reviewed by an appropriate external audit role according to a defined audit procedure for the AMI.

7.3.3 OE.InspectionSupport - Meter integrity inspections

The scheme for deployment and operation of an AMI shall include measures (based on risk-analysis) to deter tampering with the meter and to support appropriate inspections of meter integrity.

7.3.4 OE.UniqueSubjectIDs - Subjects have unique identifiers

External subjects shall use unique identifiers in their interactions with the TOE. (Note that this requirement is derived from requirement E in Smart Meter Co-ordination Group Privacy and Security Approach –Part IV.

8 Extended Components Definitions

8.1 General

In the Common Criteria it is mandatory to base requirements on components from CC Part 2 or CC Part 3 with two exceptions:

- there are security objectives for the TOE that cannot be translated to Part 2 SFRs, or there are third party requirements (e.g. laws, standards) that cannot be translated to Part 3 SARs (e.g. regarding
- evaluation of cryptography; a security objective can be translated, but only with great difficulty and/or complexity based on components in CC Part 2 and/or CC Part

In both cases the PP/ST author is required to define his own components. These defined components are called extended components. A precisely defined extended component is needed to provide context and meaning to the extended SFRs and SARs based on that component.

8.2 Security Event Alarm (FAU_ARP.2)

This component extends the existing family FAU_ARP in, adding a different type of alarm that, unlike FAU_ARP.1, is not tied directly to the audit log. Elements of definition that are relevant only to FAU_ARP.1 are not repeated here.

Family behaviour

This family defines the response to be taken in case of detected events indicative of a potential security violation.

Component levelling:



Management: FAU_ARP.2

There are no management activities defined by default.

Audit: FAU_ARP.2

There are no actions defined to be auditable by default.

FAU_ARP.2	<i>Security Event Alarm</i>
------------------	-----------------------------

Hierarchical to: No other components.

Dependencies: No dependencies

FAU_ARP.2.1	The TSF shall send an alarm message to the indicated destination for the following events: [assignment: <i>list of events and destination for the alarm for each event</i>].
FAU_ARP.2.2	The TSF shall include within each alarm message at least the following information: - Date and time of the event; - Type of event.
FAU_ARP.2.3	The TSF shall include the following additional alarm information: [assignment: <i>list of alarm messages and associated additional information</i>].
FAU_ARP.2.4	The TSF shall send alarms according to the following timing rules: [assignment: <i>rules that specify when an alarm must be sent relative to the detection of the event</i>].

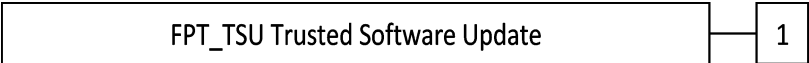
8.3 Trusted Software Update (FPT_TSU.1)

The meter firmware must be protected from tampering by an update method using digitally signed updates that can be authenticated and that have their integrity protected between the originator and the meter. A meter conformant with this PP does not allow update of any TOE firmware other than by using the secure update process.

Family behaviour

Components in this family address the requirements for trusted software/firmware update of the TSF.

Component levelling:



Management: FPT_TSU.1

There are no management activities defined by default.

Audit: FPT_TSU.1

There are no actions defined to be auditable by default.

FPT_TSU.1	<i>Trusted Software/Firmware Update</i>
------------------	---

Hierarchical to: No other components

Dependencies: FCS_COP.1

FPT_TSU.1.1	The TSF shall provide [assignment: list of authorized roles] the ability to query [selection, one of: the currently executing version of the TOE software/firmware, the currently executing and the most recently downloaded versions of the TOE software/firmware].
FPT_TSU.1.2	The TSF shall provide means to authenticate and verify the integrity of software/firmware updates to the TOE prior to installing those updates, using a digital signature mechanism that meets the following: [assignment: <i>mechanism specification</i>].
FPT_TSU.1.3	The TSF shall provide means to verify the following additional properties of software/firmware updates to the TOE prior to installing those updates: [assignment: <i>list of additional properties</i>].
FPT_TSU.1.4	The TSF shall provide [assignment: <i>list of authorized roles</i>] the ability to activate updates to TOE software/firmware.

Application note 7

In FPT_TSU.1.1 the version currently executing may not be the same as the version most recently downloaded, since a downloaded version may not yet have been activated.

The cryptographic operations used to implement the digital signature mechanism in FPT_TSU.1.2 must be specified in iterations of FCS_COP.1.

Examples of the properties specified in FPT_TSU.1.3 might be ensuring that the update is intended for the TOE type or instance or ensuring that the update is a later version than the currently executing version.

Activation in FPT_TSU.1.4 results in the updated *software/firmware* being executed.

If the TOE does not support the querying of the currently executing version, then it is legitimate to complete the assignment of the list of roles in FPT_TSU.1.1 with 'None', and in this case the SFR element is treated as trivially satisfied.

8.4 Basic TSF Self Testing (FPT_BST.1)

The extended component defined here is a simplified version of FPT_TST.1 accordance to ISO/IEC 15408-2.

Family behaviour

Components in this family address the requirements for self-testing the TSF at selected times for correct operation.

Component levelling:



Management: FPT_BST.1

There are no management activities defined by default.

Audit: FPT_BST.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Indication that TSF self-test was completed.

FPT_BST.1 Basic TSF Self Testing

Hierarchical to: No other components.

Dependencies: No dependencies.

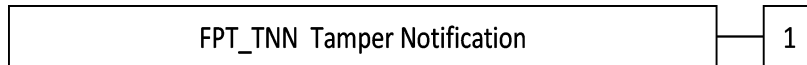
FPT_BST.1.1 The TSF shall run a suite of the following self-tests [selection: during initial start-up (on power on), periodically during normal operation, at the request of the authorized user, at the conditions [assignment: conditions under which self-tests should occur]] to demonstrate the correct operation of the TSF: [assignment: list of self-tests run by the TSF].

8.5 Tamper Notification (FPT_TNN.1)

The extended component defined here has some similarities with FPT_PHP.2 in accordance to ISO/IEC 15408-2, but states an active tamper detection requirement more suitable for devices such as smart meters.

Family behaviour

Components in this family address requirements for notification of defined tamper scenarios on identified elements of the TOE. This contrasts with FPT_PHP.1 and FPT_PHP.2 in the definition of specific tamper scenarios to be addressed, and the ability to notify using an identified interface rather than to a particular user or role.

Component levelling:**Management:** FPT_TNN.1

There are no management activities defined by default.

Audit: FPT_TNN.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- detected tampering events.

FPT_TNN.1 <i>Tamper notification</i>

Hierarchical to: No other components.

Dependencies: None

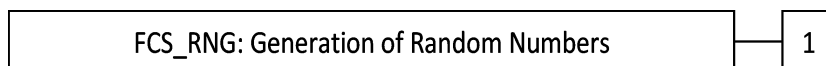
FPT_TNN.1.1 The TSF shall monitor [assignment: *list of TSF devices/elements for which active detection is required*] and notify [assignment: *designated user(s), role(s), or interface(s)*] when physical tampering of the following types has occurred: [assignment: *list of physical tampering scenarios*].

Application note 8

The second assignment ('designated user, role, or interface') describes the way in which notification is conveyed, via communication with a specific subject or else by using a particular interface (or both). The use of an interface could include, for example, a light on a device panel, the sending of a particular alarm message, or the recording of a particular log entry. In the case of a log entry, the content of the log entry should be described using an appropriate FAU SFR, and the protection of the log against modification (cf. FAU_STG.1) associated with the tamper event should be described in the TOE Summary Specification.

8.6 Generation of Random Numbers (FCS_RNG.1)**8.6.1 Family behaviour**

This family defines quality requirements for the generation of random numbers which are intended to be use for cryptographic purposes.

Component levelling:**Management:** FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no actions defined to be auditable.

FCS_RNG.1 <i>Generation of random numbers</i>
--

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RNG.1.1	The TSF shall provide a [selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic] random number generator that implements: [assignment: list of security capabilities].
FCS_RNG.1.2	The TSF shall provide [selection: bits, octets of bits, numbers [assignment: format of the numbers]] that meet [assignment: a defined quality metric].

Application note 9

A physical random number generator (RNG) produces the random number by a noise source based on physical random processes. A non-physical true RNG uses a noise source based on non-physical random processes like human interaction (key strokes). A deterministic RNG uses a random seed to produce a pseudorandom output. A hybrid RNG combines the principles of physical and deterministic RNGs where a hybrid physical RNG produces at least the amount of entropy the RNG output may contain and the internal state of a hybrid deterministic RNG output contains fresh entropy but less than the output of RNG may contain.

9 Security Requirements

9.1 Typographical Conventions

The following conventions are used in the definitions of the SFRs:

- Refinements are denoted in one of two ways, depending on whether they add detail to an SFR ('explanatory refinements') or update the text of an SFR element ('element refinements'). Explanatory refinements follow the SFR that they update and are marked by the word "Refinement" in bold followed by text describing the refinement. Element refinements are indicated by bold text within an SFR element, with the original text indicated in a footnote.
- Selections and assignments made in this PP are italicised, and the original text is indicated in a footnote. Selections and assignments that are left to be filled in by the Security Target author appear in square brackets with an indication that a selection or assignment is to be made, [selection:] or [assignment:], and the description of selection options or assignment description are *italicized*.

9.2 SFR Architecture

Figure 2 and Figure 4 give a graphical presentation of the connections between the Security Functional Requirements (SFRs) from section 9.3 and the underlying functional areas and operations that the TOE provides. The diagrams provide a context for SFRs that relates to their use in the TOE, whereas section 9.3 defines the SFRs grouped by the abstract class and family groupings in accordance to ISO/IEC 15408-2.