Protection Profile for Smart Meter Minimum Security requirements

Version: 1.0

Date: 30. October 2019

Authors: Ad-Hoc Group Privacy & Security of the CEN/CENELEC/ETSI Coordination Group on Smart Meters

Contents

1 Introduction 9

1.1 PP Reference Identification 9

1.2 PP Introduction 9

1.3 TOE Overview 10

2 Conformance Claims 12

3 Security Problem Definition 14

3.1 Assets 14

3.2 External Entities and Threat Agents 14

3.3 Threats 15

3.3.1 T.NetworkDisclosure Unauthorised data disclosure via network access 15

3.3.2 T.DirectDisclosure Unauthorised data disclosure via direct access 15

3.3.3 T.NetworkDataMod Unauthorised data modification via network access 15

3.3.4 T.DirectDataMod Unauthorised data modification via direct access 16

3.3.5 T.Malfunction Asset compromise due to TOE malfunction 16

3.4 Organisational Security Policies 16

3.4.1 P.Logging Logging security events 16

3.4.2 P.Alarms Alarms sent for critical events 16

3.5 Assumptions 17

3.5.1 A.ExternalData Protection of data outside TOE control 17

3.5.2 A.AuditSupport Audit data review 17

3.5.3 A.InspectionSupport Meter integrity inspections 17

3.5.4 A.UniqueSubjectIDs Subjects have unique identifiers 17

4 Security Objectives 18

4.1 Security Objectives for the TOE 18

4.1.1 O.Authorisation Authorisation for access to TOE data and functions 18

4.1.2 O.Messages Message protection 18

4.1.3 O.DataAtRest Stored data protection 18

4.1.4 O.Crypto Approved cryptographic mechanisms 18
4.1.5 O.Interfaces Non-operational interfaces disabled 18
4.1.6 O.Resilience Resilience against failures 18
4.1.7 O.SecureUpdate Updates protected using digital signature 19
4.1.8 O.Logging Security event logging 19
4.1.9 O.Alarms Alarms for critical events 19
4.2 Security Objectives for the Operational Environment 19
4.2.1 OE.ExternalData Protection of data outside TOE control 19
4.2.2 OE.AuditSupport Audit data review 19
4.2.3 OE.InspectionSupport Meter integrity inspections 19
4.2.4 OE.UniqueSubjectIDs Subjects have unique identifiers 19
5 Extended Components Definitions 20
5.1 Security Event Alarm (FAU_ARP.2) 20
5.2 Trusted Software Update (FPT_TSU.1) 21
5.3 Basic TSF Self Testing (FPT_BST.1) 22
5.4 Tamper Notification (FPT_TNN.1) 23
5.5 Generation of Random Numbers (FCS_RNG.1) 24
6 Security Requirements 25
6.1 Typographical Conventions 25
6.2 SFR Architecture 25
6.3 Security Functional Requirements 28
6.3.1 Cryptographic Support 28
6.3.2 User Data Protection 31
6.3.3 Identification and authentication 38
6.3.4 Protection of the TSF 40
6.3.5 Security Management 43
6.3.6 Security Audit 46
6.4 Security Assurance Requirements 49
6.4.1 Refinements of Security Assurance Requirements 50
7 Rationales 58
7.1 Security Objectives Rationale 58
7.1.1 Security Objectives Coverage 58
7.1.2 Security Objectives Sufficiency 58
7.2 Security Requirements Rationale 60

7.2.1 Security Requirements Coverage 60
7.2.2 SFR Dependencies 63
7.2.3 Rationale for SARs 66
8 References 68
Appendix A – Mapping to Minimum Security Requirements 69

Revision History

Version	Date	Description
1.0	30 Oct 2019	Updates to address NSCIB's comments dated 191029
0.91	26 Sept 2019	Updates to address Brigthsight's comments dated 190528
0.9	15 July 2019	Updates to address CEN/CENELEC comments dated 190528
1.8	30. October 2019	Updates to address CEN/CENELEC comments dated 190401.
0.7	8th November 2018	Further editorial updates to address comments. In particular, clarified that refinements to the SARs are part of the interpretation of the generic CEM work units, and not additional activities.
0.6	2nd October 2018	Further editorial updates following external commenting.
0.5	3rd May 2018	Minor editorial updates to make date information consistent and remove tamper response boundary in figure 1.
0.4	2nd May 2018	Updated draft following review and discussion (180412) at ESMIG Security and Privacy Group meeting. Changes include: • Deleted FPT_PHP.3, with tamper scenarios to be covered by updated FPT_TNN.1 and legally-based tamper seals, to more accurately reflect the real deployment scenarios • Deleted 'tamper protection boundary', requiring all debug interfaces to be disabled regardless of any such boundary • Updated FPT_TNN.1.1 to explicitly require notification of magnetic interference • Added A.InspectionSupport and OE.InspectionSupport to describe the assumption that all deployed meters will have specific risk-analysed measures in place to deter tampering and support appropriate inspections of meter integrity.
0.3	6th April 2018	Updated draft following review and discussion (180320-22) with ESMIG subgroup. Changes include: • Replaced FPT_PHP.2 with extended SFR FPT_TNN.1

		• Added Glossary entries for LAN, local network, neighbourhood network, consumer • Changed 'tamper boundary' to 'tamper protection boundary' and updated definition • Figure 1 updated to show functional reference architecture interface labels and non-TSF parts; note added to refinement of ADV_FSP.3 that internal interfaces may be classed as 'inaccessible' • Changed 'Local' to 'Direct' in the context of the non-network connections to the meter. This includes changing the names of relevant threats. • Similarly changed 'Remote' to 'Network'. • Added mapping table to Minimum Requirements as Appendix A
0.2	23rd February 2018	Updated draft following review and discussion (180115) with ESMIG subgroup. Changes include: • Added note that the CC requirements have added specific detail to the minimum requirements, and specific evaluation activity requirements (section 1.2) • Added footnotes to discuss potential variation in the detailed composition of display and keypad interfaces (section 1.3) • Added auditing of detected replay events (FAU_GEN.1) • Removed auditing of key destruction (FAU_GEN.1) • Removed auditing of RBG instantiation/reseeding (FAU_GEN.1) • Added flaw remediation procedures within the scope of the evaluation – note that this is over and above the requirements in [5] (ALC_FLR.3) • Added manufacturing environment security aspects within the scope of the evaluation – note that this is over and above the requirements in [5] (ALC_DVS.1) • Added definition of "Digital Signature" to clarify that this requires a cryptographic mechanism (Glossary) • Added definition of "operational interfaces" (Glossary) • Added refinement of ASE_REQ.2 (section 6.4.1)
0.1	20th December 2017	First draft for comment

Glossary

Term	Meaning
Administrator	Entity that has a level of trust with respect to all policies implemented by the TSF – see [1]. The Administrator role is referred to in SFRs in section 6.3 as a generic terms for a privileged role that has access to sensitive operations affecting the configuration and operation of the meter.
AMI **Advanced Metering Infrastructure**	Infrastructure which allows two way communications between the Head-End System and the meter(s) and may be linked to other in-house devices.
Assurance	Grounds for confidence that a TOE meets the SFRs – see [1].
Consumer	End user of the metered quantity (electricity, gas, water or thermal energy)
Critical Event	An event that can take place in a smart meter and that is particularly significant for supply or security of the meter. (The critical events for a meter conformant with this Protection Profile are defined as part of FAU_ARP.2 in section 6.3.6.1.)
Digital Signature	A cryptographic digital signature applied to data in order to allow verification of its integrity and authenticity.
Direct Interface	An interface to the meter that does not involve access from external networks (WAN, Neighbourhood Network or Local Network).
EM	Electromagnetic
EU	European Union
Evaluator	The person or group that carries out a security evaluation of the TOE, using the criteria in [1], [2] and [3] and the associated methodology in [4].
External Entity	See 'User'.

Term	Meaning
Firmware	Executable code of a meter that is stored in hardware and that cannot be updated except via a secure update process (for the purposes of this Protection Profile the relevant update process is defined in FPT_TSU.1, see section 6.3.4.6).
Hand-Held Terminal Unit	Portable device for reading and programming equipment or meters at the consumer's premises or at the access point – see [6]
JTAG	The name (adapted from 'Joint Test Action Group') commonly used to refer to the interface defined in IEEE 1149.1 Standard Test Access Port and Boundary-Scan Architecture.
Local Network	Data communication network providing access to local (in-house/building) devices and / or other local networks – see [6].
MAC **Message Authentication Code**	A 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).
Message	The term 'message' is generally used in this Protection Profile to refer to application-level messages. The minimum requirements in [5] 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.
Meter data	Meter readings that allow calculation of the quantity of electricity, gas, water or thermal energy consumed over a period. 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) – see [6].
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)
MID	Measuring Instruments Directive 2014/32/EU
Neighbourhood Network	Data communication network providing access to several premises and / or other neighbourhood networks – see [6]

Term	Meaning
Operational Interfaces	Interfaces required for normal operation of the meter (all other accessible interfaces are disabled)
PP **Protection Profile**	Implementation-independent statement of security needs for a TOE type – see [1].
Role	The entitlement of a party to execute a set of one or more commands associated with the role name. (Note that this is different to the definition in [1], but consistent with the interpretation and refinement of "role" in this PP.)
SAR **Security Assurance Requirement**	A description of how the TOE is to be evaluated, using the standardised language of [3] – see section A.9.2 of [1].
SFR **Security Functional Requirement**	A translation of the security objectives for the TOE into a set of standardised functional requirements drawn from [2] (or as extended components, cf. section 8.3 of [1]) – see section A.9.1 of [1].
Sensor	Device that translates a physical property in an electric signal. A sensor can be a non TSF part of the TOE, or mounted externally, for example a current transformer or a temperature sensor on a water return pipe.
Service Technician	Users who carry out any local installation, commissioning, maintenance or diagnostic activities on a meter. These activities may be carried out over direct or network interfaces and service technicians may need access to privileged functions.
SM-CG	Smart Meters Co-ordination Group A 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.
ST **Security Target**	Implementation-dependent statement of security needs for a specific identified TOE – see [1].
TOE **Target of Evaluation**	A set of software, firmware and/or hardware possibly accompanied by guidance – see [1].

Term	Meaning
TSF **TOE Security Functionality**	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs – see [1].
TSF Data	Data for the operation of the TSF upon which the enforcement of the requirements relies – see [1].
User	Human or IT entity interacting with the TOE from outside of the TOE boundary (based on [1]).
WAN **Wide Area Network**	extended data communication network connecting a large number of communication devices over a large geographical area – see [6]

See [1] for other Common Criteria abbreviations and terminology.

1 Introduction

1.1 PP Reference Identification

PP Reference: Protection Profile for Smart Meter Minimum Security requirements

PP Version: 1.0

PP Date: 30. October 2019

1.2 PP Introduction

This Protection Profile describes a set of security requirements for smart meters, based on the 'minimum security requirements' for components of AMI infrastructures in [5]. The requirements in [5] were 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 SCG-SM[1] Task Force on Privacy and Security have 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

[1] CEN/CENELEC/ETSI Coordination Group on Smart Meters

Requirements (SFRs) and refinements to the Security Assurance Requirements (SARs)[2]. 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 PP is to come to an European approach for the security certification of Smart Meters. The Cyber Security Act of the European Commission, that comes 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 recognises however 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 WG 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 Common Criteria (see [1]). Sections 1 – 4 are 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 [1], [2] and [3] – 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.

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

1.3 TOE Overview

The TOE is a smart supply meter that monitors, and possibly limits, the consumption of electricity, gas, thermal energy or water[3] provided by utilities supply markets and communicates with users via

[2] 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.

[3] Exhaustive list which matches the main media types in the OBIS identification system.

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 figure 2 in [6][4].)

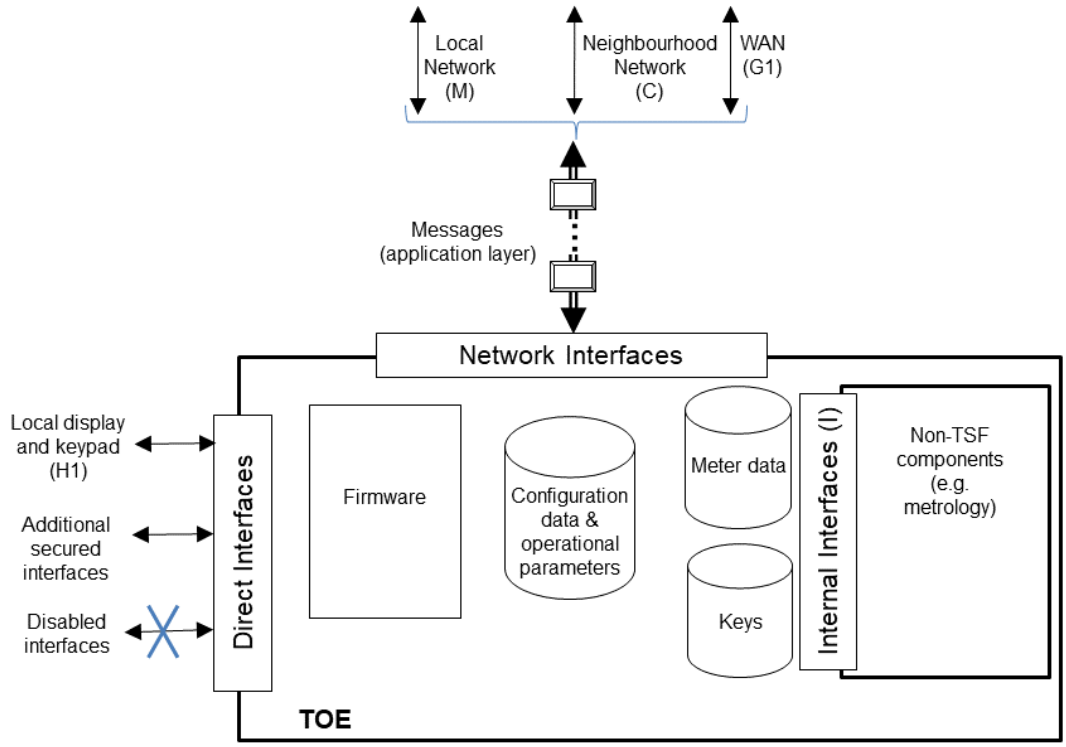


Figure 1 - Generic Smart Meter TOE Architecture

The TOE provides a combination of the following meter-related functions from the reference architecture in [6]:

- 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

[4] The 'additional secured interfaces' do not have a specific mapping to [6] and are defined specifically for each meter – cf. FDP_IFF.1/Int.

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[5] and keypad[6] for interaction with the user, and other communication interfaces (e.g. H1, H2 in [6]). 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 portable device for reading and programming meters at the consumer's premises).

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 may have a physical presence on the meter (such as an optical port or debug interface) or may 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.

2 Conformance Claims

As defined by the references [1], [2] and[3], this PP:

[5] The meter display may include a number of separate elements, such as one or more LCD panels and LED lights, but are treated as a single type of interface for the purposes of this description. If different security requirements apply to different elements of the display then this should be explained in the Security Target.

[6] As with the display, the keypad may comprise a number of input elements but these are treated as a single type of interface for the purposes of this description. A keypad may also consist of a single button in some cases. If different security requirements apply to different elements of the keypad interface then this should be explained in the Security Target.

- conforms to the requirements of Common Criteria v3.1, Revision 5
- is Part 2 extended, Part 3 conformant
- 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.

3 Security Problem Definition

3.1 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 is 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 data[7].

This Protection Profile does not define specific types of sensitive personal information or personally identifiable information. 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 confidentiality, integrity and authenticity of such information are to be included in the specific authorisation, access control and data destruction rules defined in a Security Target[8].

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.

3.2 External 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.

[7] 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.
[8] 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.

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 Target[9]. As an example, one such role might be that of a service technicians 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.

3.3 Threats

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 authorised 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 3.2 (but in this case the attacker will not have access to the authentication or authorisation data for the user or remote entity).

3.3.1 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/authorisation 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 authorisation) to remotely access data stored in the TOE.

3.3.2 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 authorisation) via a direct interface to access data stored in the TOE (noting that, in additional 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).

3.3.3 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 authorisation 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

[9] 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.

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 authorisation) to remotely modify data stored in the TOE.

3.3.4 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 authorisation for modification (defined according to the policies implemented in the meter). The scope of such data is 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 authorisation) via a direct interface to modify data stored in the TOE (noting that, in additional 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).

3.3.5 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 realised.

3.4 Organisational Security Policies

The TOE shall comply with the following organisational security policies.

3.4.1 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.

3.4.2 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[10]*.*

[10] The definition of the events is required in FAU_ARP.2.

3.5 Assumptions

3.5.1 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.

3.5.2 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.

3.5.3 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.

3.5.4 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 [5].)

4 Security Objectives

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.

4.1 Security Objectives for the TOE

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

4.1.1 O.Authorisation Authorisation for access to TOE data and functions

The TOE shall check the authorisation 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 authorisation attempts by temporarily denying all further authorisation requests for a defined period of time. Successful authorisation attempts shall expire after a defined period of time.

4.1.2 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.

4.1.3 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.

4.1.4 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).

4.1.5 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.

4.1.6 O.Resilience Resilience against failures

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

4.1.7 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 meter. The secure update function applies to all firmware in the TOE that can be updated.

4.1.8 O.Logging Security event logging

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

4.1.9 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.

4.2 Security Objectives for the Operational Environment

The following security objectives relate to the TOE environment.

4.2.1 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.

4.2.2 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.

4.2.3 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.

4.2.4 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 [5].)

5 Extended Components Definitions

5.1 Security Event Alarm (FAU_ARP.2)

This component extends the existing family FAU_ARP in [2], adding a different type of alarm that, unlike FAU_ARP.1, is not tied directly to the audit log. Note that 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	*Security Event Alarm*
	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: *list of events and destination for the alarm for each event*].
FAU_ARP.2.2	The TSF shall include within each alarm message at least the following information: a) Date and time of the event; b) Type of event.
FAU_ARP.2.3	The TSF shall include the following additional alarm information: [assignment: *list of alarm messages and associated additional information*].

FAU_ARP.2.4	The TSF shall send alarms according to the following timing rules: [assignment: *rules that specify when an alarm must be sent relative to the detection of the event*].

5.2 Trusted Software Update (FPT_TSU.1)

Family behaviour

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

Component levelling:

FPT_TSU Trusted Software Update	1

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 *Trusted Software/Firmware Update*

Hierarchical to: No other components

Dependencies: FCS_COP.1

FPT_TSU.1.1	The TSF shall provide [assignment: *list of authorised 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*: mechanism specification*].
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*: list of additional properties*].
FPT_TSU.1.4	The TSF shall provide [assignment: *list of authorised roles*] 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.

5.3 Basic TSF Self Testing (FPT_BST.1)

The extended component defined here is a simplified version of FPT_TST.1 in [2].

Family behaviour

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

Component levelling:

FPT_TST_EXT Basic TSF Self Testing	1

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 authorised 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*].

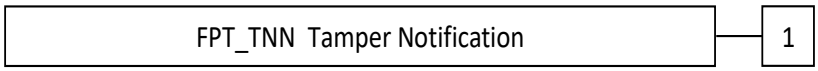
5.4 Tamper Notification (FPT_TNN.1)

The extended component defined here has some similarities with FPT_PHP.2 in [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	*Tamper notification*
	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.

5.5 Generation of Random Numbers (FCS_RNG.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:

FCS_RNG: Generation of Random Numbers	1

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	*Generation of random numbers*
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, mouse movement). 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.

6 Security Requirements

6.1 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*.

6.2 SFR Architecture

Figure 2 and Figure 4 give a graphical presentation of the connections between the Security Functional Requirements (SFRs) from section 6.3 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 6.3 defines the SFRs grouped by the abstract class and family groupings in [2].

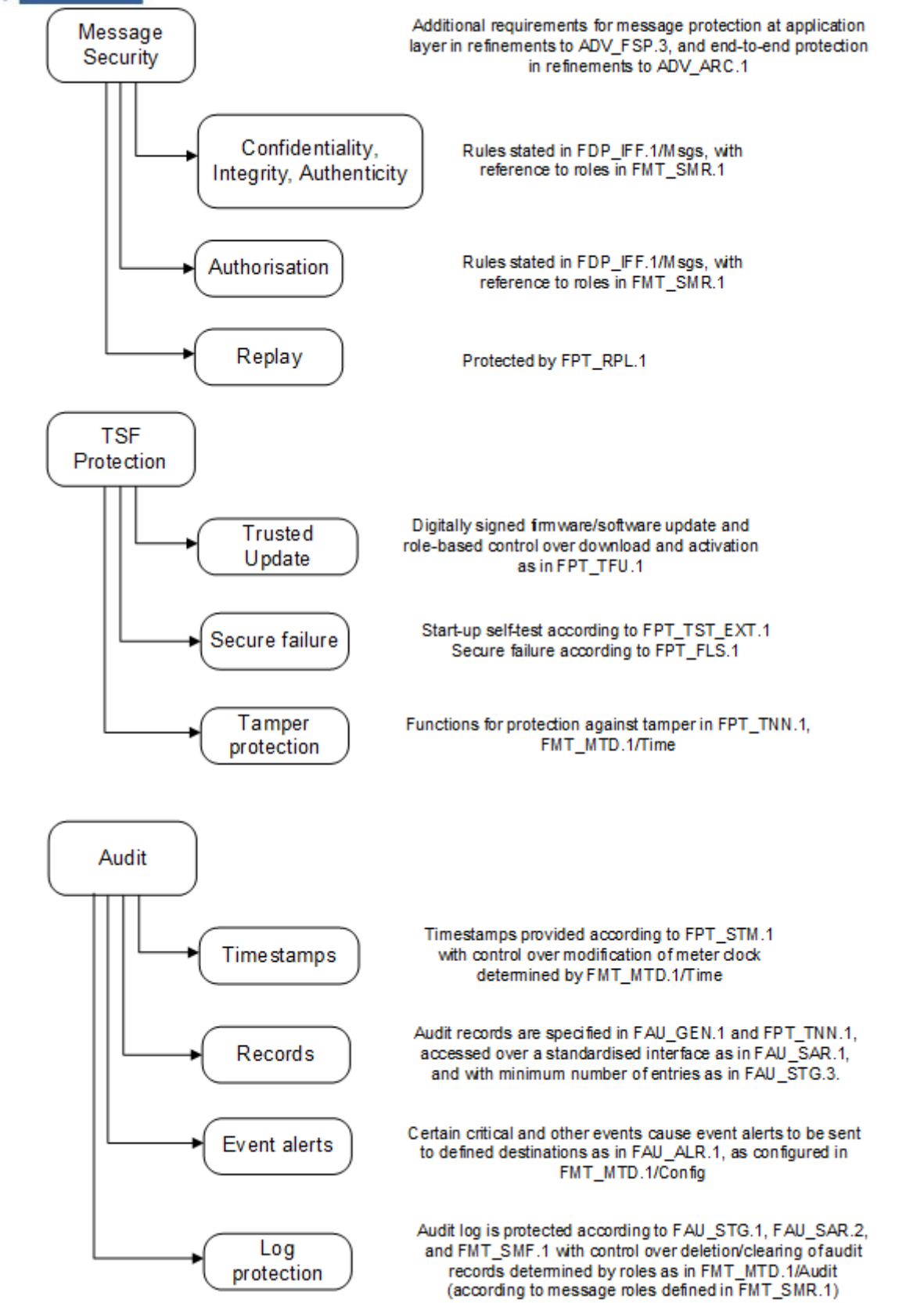

Message Security
Additional requirements for message protection at application layer in refinements to ADV_FSP.3, and end-to-end protection in refinements to ADV_ARC.1
Confidentiality, Integrity, Authenticity
Rules stated in FDP_IFF.1/Msgs, with reference to roles in FMT_SMR.1
Authorisation
Rules stated in FDP_IFF.1/Msgs, with reference to roles in FMT_SMR.1
Replay
Protected by FPT_RPL.1
TSF Protection
Trusted Update
Digitally signed firmware/software update and role-based control over download and activation as in FPT_TFU.1
Secure failure
Start-up self-test according to FPT_TST_EXT.1 Secure failure according to FPT_FLS.1
Tamper protection
Functions for protection against tamper in FPT_TNN.1, FMT_MTD.1/Time
Audit
Timestamps
Timestamps provided according to FPT_STM.1 with control over modification of meter clock determined by FMT_MTD.1/Time
Records
Audit records are specified in FAU_GEN.1 and FPT_TNN.1, accessed over a standardised interface as in FAU_SAR.1, and with minimum number of entries as in FAU_STG.3.
Event alerts
Certain critical and other events cause event alerts to be sent to defined destinations as in FAU_ALR.1, as configured in FMT_MTD.1/Config
Log protection
Audit log is protected according to FAU_STG.1, FAU_SAR.2, and FMT_SMF.1 with control over deletion/clearing of audit records determined by roles as in FMT_MTD.1/Audit (according to message roles defined in FMT_SMR.1)

Figure 2: Architecture of Message Security, TSF Protection and Audit SFRs

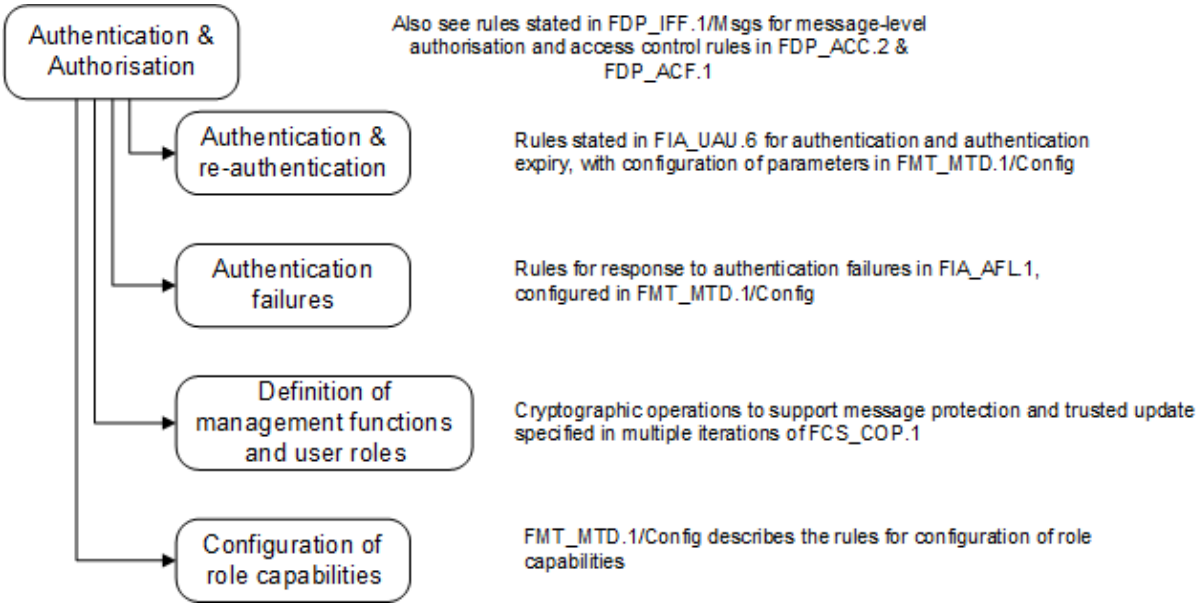


Figure 3: Architecture of Authentication & Authorisation SFRs

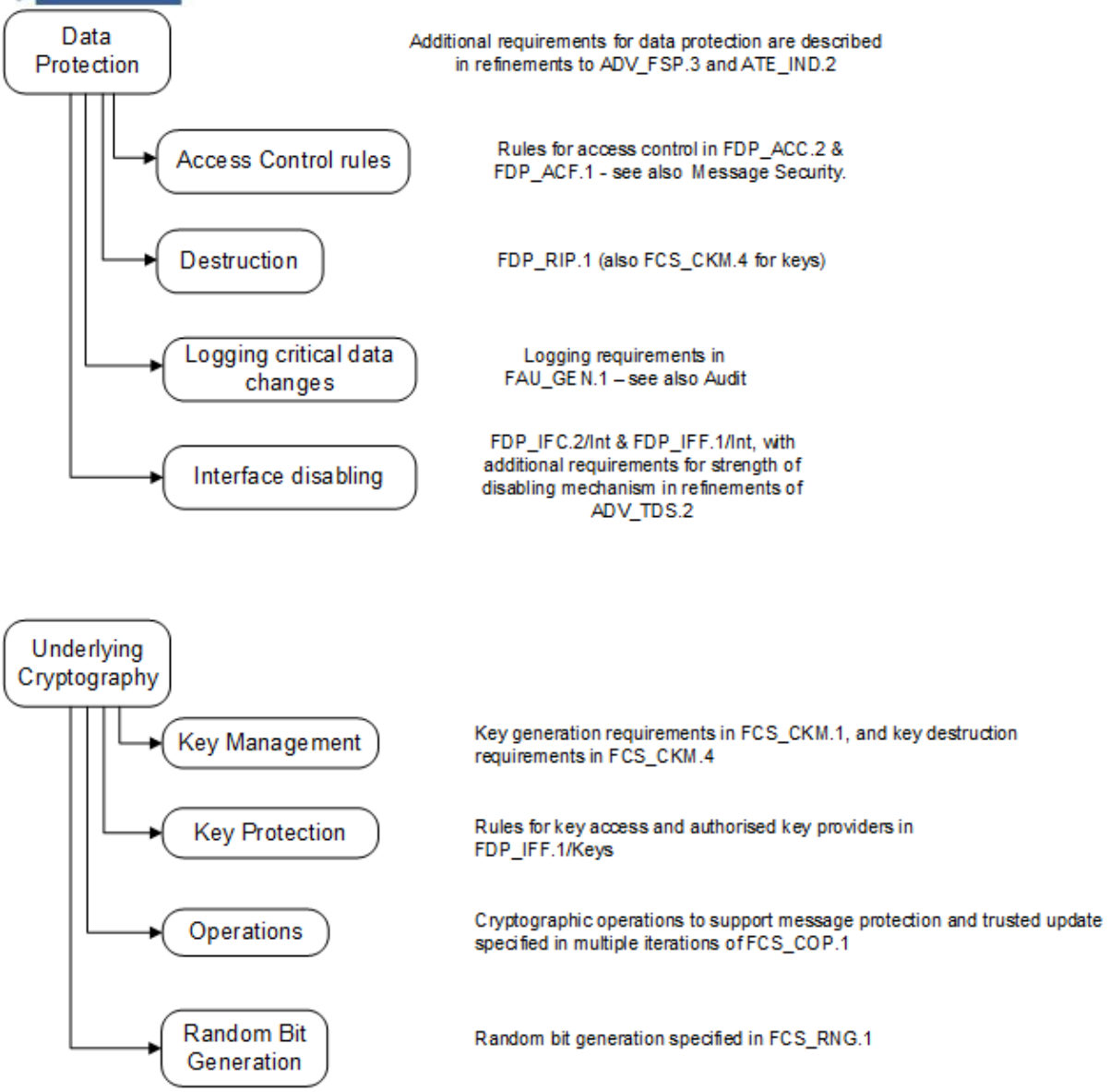


Figure 4: Architecture of Data Protection and Underlying Cryptography SFRs

6.3 Security Functional Requirements

The individual security functional requirements are specified in the sections below.

6.3.1 Cryptographic Support

6.3.1.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1	*Cryptographic key generation*

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment*: cryptographic key sizes*] that meet the following: [assignment*: list of standards*].

Application Note 10

The Security Target must include an iteration of FCS_CKM.1 for each cryptographic key that is generated in the meter and supports other parts of the TSF (e.g. message protection (see FDP_IFF.1/Msgs in section 6.3.2.4)). The ST author identifies where the random bit generator specified by FCS_RNG.1 is used for key generation.

If the meter does not generate any keys then the ST author completes all of the assignments with 'None' and addresses the import of keys using the rules in FDP_IFF.1/Keys (see also the requirements for description of security-related activities in the manufacturing environment as part of the refinements to ALC_DVS.1 in section 6.4.1.6). Where this import relies on a secure channel the ST author also adds a secure channel SFR to describe this channel (see the discussion of secure channel SFRs in Application Note 17).

6.3.1.2 Cryptographic key destruction (FCS_CKM.4)

FCS_CKM.4 *Cryptographic key destruction*

Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment*: cryptographic key destruction method*] that meets the following: [assignment*: list of standards*].

Application Note 11

The Security Target must specify the method(s) of secure destruction of all private and secret keys that it holds (whether they were generated internally or received from some other source). If necessary then more than one iteration of FCS_CKM.4 may be included to describe different standards for secure deletion. The 'list of standards' in the final assignment may be met in the Security Target by simply providing a description of the action taken to destroy the keys rather than referencing an external standard.

6.3.1.3 Cryptographic operation (FCS_COP.1)

FCS_COP.1 *Cryptographic operation*

Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1	The TSF shall perform [assignment: *list of cryptographic operations*] in accordance with a specified cryptographic algorithm [assignment*: cryptographic algorithm*] and cryptographic key sizes [assignment*: cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

Application Note 12

The Security Target must include an iteration of FCS_COP.1 for each cryptographic operation that supports message protection (see FDP_IFF.1/Msgs in section 6.3.2.4). For example, separate iterations would be used to describe the cryptographic functions used for digital signature (e.g. to support authentication and authorisation mechanisms), and for confidentiality. In addition, iterations of FCS_COP.1 must be included for each cryptographic operation used to support trusted update (see FPT_TSU.1 in section 6.3.4.6) – examples here would include digital signature, confidentiality, and also any separate hash mechanism used to protect the update.

Approved cryptographic standards are determined by the relevant authority for an AMI.

6.3.1.4 Generation of random numbers (FCS_RNG.1)

FCS_RNG.1	*Generation of random numbers*

Dependencies:	No dependencies.
FCS_RNG.1.1	The TSF shall provide a [selection: *physical, 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 13

A physical random number generator (RNG) – also referred to as a random bit generator (RBG) – produces the random number by a noise source based on physical random processes. 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.

The ST author describes the ways in which random numbers generated according to FCS_RNG.1 are used by the TOE in the TOE Summary Specification. Examples of such uses would be generation of cryptographic keys or challenges.

6.3.2 User Data Protection

6.3.2.1 Complete access control (FDP_ACC.2)

FDP_ACC.2	*Complete access control*

Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.2.1	The TSF shall enforce the *Meter Data SFP*[11] on *(1) subjects: all* *(2) objects: metrologically certified data, credentials, meter configuration, [assignment: other controlled meter data items]*[12] and all operations among subjects and objects covered by the SFP.
FDP_ACC.2.2	The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Application Note 14

The ST author describes and explains the specific implementation of the controlled objects, including 'metrologically certified data', 'credentials', and 'meter configuration' in the Security Target and this is also described and explained in the operational guidance for the meter with reference to the actual terminology and names of objects in that particular meter (cf. refinement of AGD_OPE.1 in section 6.4.1.5).

6.3.2.2 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1	*Security attribute based access control*

Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1	The TSF shall enforce the *Meter Data SFP*[13] to objects based on the following: *(1) Metrologically certified data (e.g. consumption/generation measurements)* *(2) Credentials* *(3) Meter configuration* *(4) [assignment: list other of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security*

[11] [assignment: *access control SFP*]
[12] [assignment: *list of subjects and objects*]
[13] [assignment: *access control SFP*]

attributes, or named groups of SFP-relevant security attributes][14].

Application Note 15

Authorisation of a subject for access to the objects in FDP_ACF.1.1 is defined in the rules in the other elements of FDP_ACF.1 below – these exclude rules for accesses via messages which are separately described in FDP_IFF.1/Msgs. The rules therefore apply, for example, to the meter's user interface. The rules describe the role- and/or identity-based access controls to objects that are used to enforce appropriate protection based on a risk analysis.

FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

Application Note 16

Note that the security policy for access to cryptographic keys is described separately in FDP_IFF.1/Keys. In most cases it is expected that the keys will be accessed via messages (and therefore will be subject to FDP_IFF.1/Msgs as well as FDP_IFF.1/Keys); however if non-message interfaces also provide access to keys then there may also be relevant rules included in FDP_ACF.1 and FDP_IFF.1/Keys.

6.3.2.3 Subset information flow control (FDP_IFC.1) – Messages

FDP_IFC.1/Msgs	*Subset information flow control*

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1/Msgs The TSF shall enforce the *Messages SFP*[15] on

(1) subjects: all

(2) information: messages

(3) operations: send, receive[16].

[14] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

[15] [assignment: *information flow control SFP*]

[16] [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*]

6.3.2.4 Simple security attributes (FDP_IFF.1) - Messages

FDP_IFF.1/Msgs	*Simple security attributes*

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1/Msgs The TSF shall enforce the *Messages SFP*[17] based on the following types of subject and information security attributes: *[assignment: list of message types and any other message attributes that determine the protection measures to be applied according to the rules below]*[18].

FDP_IFF.1.2/Msgs The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *for each operation and message type, a list of the confidentiality protection, integrity protection, authentication protection, and authorisation rules applicable to the message type*][19].

FDP_IFF.1.3/Msgs The TSF shall enforce the **following additional information flow control rules**[20]**:** [assignment: *additional information flow control SFP rules*].

FDP_IFF.1.4/Msgs The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly authorise information flows*].

FDP_IFF.1.5/Msgs The TSF shall explicitly deny an information flow based on the following rules:

(1) Message received from a source that is not authorised to send messages of that type;

(2) [assignment: other rules, based on security attributes, that explicitly deny information flows][21].

Application Note 17

The ST must describe the types of messages and the policy for protection of each message type using this SFR. In most cases the rules for message types can probably be expressed using FDP_IFF.1.1 and FDP_IFF.1.2 only, in which case the assignments in FDP_IFF.1.3, FDP_IFF.1.4 and FDP_IFF.1.5 can be completed with 'none' (in the case of FDP_IFF.1.5 the 'none' can be omitted, leaving only rule (1)).

The operations referred to in FDP_IFF.1.2/Msgs are those defined in FDP_IFC.1/Msgs, and the messages covered by the operations and rules include security event alarms as described in FAU_ARP.2 (section 6.3.6.1).

[17] [assignment: *information flow control SFP*]

[18] [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]

[19] [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]

[20] This refinement is applied to improve readability of the SFR element.

[21] [assignment: *rules, based on security attributes, that explicitly deny information flows*]

The term "authorisation measures" in FDP_IFF.1.2 means measures that determine whether or not a source is authorised to provide certain message types to the meter (note that this may overlap with authorisation of sources of imported keys in FDP_IFF.1.2/Keys and with authentication in FIA_UAU.6 and FIA_AFL.1). In general, these authorisation rules would be expected to use the roles defined in FMT_SMR.1 (section 6.3.5.1). The authorisation measures stated in these rules might, for example, define an implementation of role-based permissions to limit certain message types to energy suppliers or network operators. Although no specific authorisation measures are stated in this PP, it is expected that every meter conformant to this PP will define some authorisation measures in its ST, and this is expressed by the general 'deny' rule in FDP_IFF.1.5/Msgs.

An example of a rule that could be stated in FDP_IFF.1.2/Msgs would be "All commands, responses and alarms in the 'Critical' group (as defined in <reference>) shall be discarded without effect unless the digital signature (as defined in <reference>) is valid and belongs to a role that is authorised to issue the message according to <reference>" – in this case references would be given (in the SFR or using application notes in the ST) to the definition of the 'Critical' message group, the format and creation of the digital signature, and the definition of permitted messages for each role.

The rules expressed in FDP_IFF.1/Msgs must make clear how the access controls over types of data defined in FDP_ACF.1 are implemented for message processing (cf. the refinement of ADV_ARC.1 in section 6.4.1.2). The references might be to other rules listed in the SFR, or to external documents, however it is important that the references define unambiguous rules that can therefore be tested (cf. the refinement of ATE_IND.2 in section 6.4.1.7).

The rules must cover all available combinations of messages and interfaces over which they can be sent. Thus, for example, a message that can be received from any of the Local Network, Neighbourhood Network, or WAN, must specify the protection applicable to each of the interfaces. At the level of direct interfaces this would include interfaces such as using inter-PAN on a ZigBee TOE to communicate directly with a device such as a hand-held terminal unit.

The ST author may introduce additional iterations of FDP_IFF.1/Msgs (e.g. appending the name of the interface or protocol as the iteration name) in order to specify separate rules applicable to each interface.

Rules governing authorised access to objects other than via messages are given in FDP_ACF.1. As part of the refinement of ADV_FSP.3 in section 6.4.1.3 the evaluator checks that the rules given in the Meter Data SFP (FDP_ACF.1), Messages SFP (FDP_IFF.1/Msgs), and the Keys SFP (FDP_IFF.1/Keys) are unambiguous and completely cover the interfaces, operations and data provided by the TOE.

The ST author describes the protection specified for messages in terms of cryptographic operations defined in iterations of FCS_COP.1 (see section 6.3.1.3).

Where the protection of messages is based on a secure channel rather than by protecting each individual message (noting that security measures are required to be implemented at the application layer and not to depend on the lower layer protocols, as checked in the refinements to ADV_FSP.3 in section 6.4.1.3) then the ST author should consider adding an SFR to describe the secure channel used (e.g. FDP_ITC.1 or FTP_ITC.1).

Note that if the TOE receives random bits that support SFRs (e.g. for generation of keys, nonces or salts), or if it receives keys rather than generating its own, then the rules in FDP_IFF.1/Msgs must include the specification of the secure channel(s) used to transmit the random bits and/or keys. In the case of receiving random bits and/or keys from other AMI components, these rules should be supported by inclusion of a secure channel SFR (such as FDP_ITC.1 or FTP_ITC.1) in the Security Target.

6.3.2.5 Complete information flow control (FDP_IFC.2) – Interfaces

FDP_IFC.2/Int *Complete information flow control*

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1/Int The TSF shall enforce the *Interfaces SFP*[22] on

(1) subjects: all

(2) information: all communication[23]

and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2/Int The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

6.3.2.6 Simple security attributes (FDP_IFF.1) - Interfaces

FDP_IFF.1/Int *Simple security attributes*

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1/Int The TSF shall enforce the *Interfaces SFP*[24] based on the following types of subject and information security attributes: *[assignment: list of logical and physical interfaces presented]*[25].

FDP_IFF.1.2/Int The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation **only via the following interfaces**[26]: [assignment: *for each enabled interface presented, a statement of the operational use of the interface*][27].

FDP_IFF.1.3/Int The TSF shall enforce the **following additional information flow control rules**[28]: *None*[29].

FDP_IFF.1.4/Int The TSF shall explicitly authorise an information flow based on the following rules: *None*[30].

---

[22] [assignment: *information flow control SFP*]
[23] [assignment: *list of subjects and information*]
[24] [assignment: *information flow control SFP*]
[25] [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]
[26] if the following rules hold
[27] [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]
[28] This refinement is applied to improve readability of the SFR element.
[29] [assignment: *additional information flow control SFP rules*]
[30] [assignment: *rules, based on security attributes, that explicitly authorise information flows*]

FDP_IFF.1.5/Int	The TSF shall explicitly deny an information flow based on the following rules: *(1) any interface other than those in FDP_IFF.1.2/Int is disabled*][31].

Application Note 18

The purpose of this SFR is to ensure that If the device has interfaces other than those supporting normal operation (and that are therefore not necessarily governed by the access control rules in FDP_IFF.1/Msgs or other SFRs – e.g. debug interfaces or other interfaces intended for use during manufacturing), then these interfaces are disabled for normal operation. FDP_IFF.1.1/Int therefore lists the available operational interfaces (i.e. those required for normal operation), and FDP_IFF.1.5/Int requires that all other accessible interfaces are disabled. Note that these operational interfaces are defined at the level of protocols and available commands, and not simply at a general level such as WAN, Neighbourhood Network or Local Network. A refinement of ADV_TDS.2 in section 6.4.1.4 requires that the disabled interfaces and their methods of disablement are documented and examined by the evaluators. Methods of disabling the interfaces may be physical (e.g. based on manufacturing actions) or logical (e.g. by requiring authentication of at least the same strength as for FIA_UAU.6 or for support of other protection mechanisms over messages (FDP_IFF.1/Msgs), meter data (FDP_ACF.1) or keys (FDP_IFF.1/Keys)).

The Functional Specification describes the interfaces that are presented by the TOE). Some of these interfaces are used for the normal operation of the meter, and all others are disabled: this is identified by the ST author in FDP_IFF.1.2/Int. Note that 'normal operation' of the meter here includes any interfaces that require authentication and that may be limited to specific roles (e.g. administration or maintenance roles). For the disabled interfaces, the Functional Specification describes the method(s) by which these interfaces are disabled – including both physical and logical methods as appropriate. This is supported by the analysis of design elements and testing of the post-installation state required by the refinements of the assurance requirements in section 6.4.1.

6.3.2.7 Subset information flow control (FDP_IFC.1) – Keys

FDP_IFC.1/Keys	*Subset information flow control*
Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.1.1/Keys	The TSF shall enforce the *Keys SFP*[32] on *(1) subjects: all* *(2) information: keys* *(3) operations: send, import*[33].

[31] [assignment: *rules, based on security attributes, that explicitly deny information flows*]
[32] [assignment: *information flow control SFP*]
[33] [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*]

6.3.2.8 Simple security attributes (FDP_IFF.1) - Messages

FDP_IFF.1/Keys	*Simple security attributes*

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1/Keys The TSF shall enforce the *Keys SFP*[34] based on the following types of subject and information security attributes: *[assignment: list of key types and any attributes that determine the protection measures to be applied according to the rules below]*[35].

FDP_IFF.1.2/Keys The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *for each operation and key type, a list of the confidentiality protection, integrity protection, authentication protection, and authorisation measures applicable to the key type*][36].

FDP_IFF.1.3/Keys The TSF shall enforce the **following additional information flow control rules[37]:** [assignment: *additional information flow control SFP rules*].

FDP_IFF.1.4/Keys The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly authorise information flows*].

FDP_IFF.1.5/Keys The TSF shall explicitly deny an information flow based on the following rules:

(1) *A key received from a source that is not authorised to provide keys of that type shall be rejected;*

(2) *No read access shall be provided to plaintext private or secret keys stored in the meter;*

(3) *[assignment: other rules, based on security attributes, that explicitly deny information flows]*[38].

Application Note 19

The ST describes the types of keys and the policy for protection of each key type using this SFR. In most cases the rules for key types can probably be expressed using FDP_IFF.1.1 and FDP_IFF.1.2 only, in which case the assignments in FDP_IFF.1.3, FDP_IFF.1.4 and FDP_IFF.1.5 can be completed with 'none'.

The operations referred to in FDP_IFF.1.2/Keys are those defined in FDP_IFC.1/Keys.

---

[34] [assignment: *information flow control SFP*]

[35] [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]

[36] [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]

[37] This refinement is applied to improve readability of the SFR element.

[38] [assignment: *rules, based on security attributes, that explicitly deny information flows*]

The term "authorisation measures" in FDP_IFF.1.2 means measures that determine sources that are authentic and authorised to provide keys to the meter (note that this may overlap with authorisation of sources of particular message types in FDP_IFF.1.2/Msgs and with authentication in FIA_UAU.6 and FIA_AFL.1). In general these authorisation rules would be expected to use the roles defined in FMT_SMR.1 (section 6.3.5.1). Although no specific authorisation measures are stated in this PP, it is expected that every meter conformant to this PP will define some authorisation measures in its ST, and this is expressed by the general 'deny' rule in FDP_IFF.1.5/Keys.

Examples of rules that could be stated in FDP_IFF.1.2/Keys would be "All public keys generated in the TOE are exported in the form of a certificate signing request", and "Public keys for eternal entities shall only be imported into the TOE in the form of a public key certificate validated as defined in <reference> and received from a source authenticated as defined in <reference> and where the source has a role that is authorised to issue the key according to <reference>". In this case the references might be to other rules listed in the SFR, or to external documents, however it is important that the references define unambiguous rules that can therefore be tested (cf. the refinement of ATE_IND.2 in section 6.4.1.7).

The 'deny' rule in FDP_IFF.1.5/Keys item (2) ensures that there is no way to read unencrypted secret or private keys over any interface of the TOE.

The import rules must cover all relevant secret, private and public keys.

Requirements for the documentation of keys are included in the refinements of ADV_FSP.3 and ADV_TDS.2 in section 6.4.1.

6.3.2.9 Subset residual information protection (FDP_RIP.1)

FDP_RIP.1	*Subset residual information protection*

Dependencies: No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from*[39] the following objects: [assignment: *list of objects*].

Application Note 20

Note that destruction of cryptographic keys is also subject to the requirements of FCS_CKM.4.

The objects listed in FDP_RIP.1.1 include those objects that are subject to the access control rules in FDP_ACF.1. 'Deallocation of the resource' means that the objects are made unavailable as soon as a deletion or replacement of the object takes place.

6.3.3 Identification and authentication

6.3.3.1 Re-authenticating (FIA_UAU.6)

FIA_UAU.6	*Re-authenticating*

Dependencies: No dependencies.

[39] [selection: *allocation of the resource to, deallocation of the resource from*]

FIA_UAU.6.1 The TSF shall re-authenticate **authenticate and re-authenticate**[40] the user **for access to data** under the conditions *defined in the Re-authentication Table*[41].

ID	Data	Authentication for initial access	Re-authentication
(i)	*[assignment: types of data]*	*[assignment: method of authentication]*	*After a period of [assignment: time period] from the previous successful authentication*

Table 1: Re-authentication Table

Application Note 21

This SFR requires user authentication for access to all types of data held on the TOE. If necessary, different types of data with different authentication methods and re-authentication times, may be specified using separate rows in the Re-authentication Table, provided that all types of data are covered by the complete set of rows.

This SFR also covers authentication over all available interfaces: separate rows in the Re-authentication Table may also be used to distinguish interfaces and the types of data they give access to).

If the period of time for reauthentication is configurable then the roles that are able to configure this are specified in FMT_MOF.1.

6.3.3.2 Failure with preservation of secure state (FIA_AFL.1)

FIA_AFL.1 *Authentication failure handling*

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when *an administrator configurable positive integer within the range in the Authentication Failure Handling Table*[42] **of** unsuccessful authentication attempts occur related to *consecutive failed authentication attempts for access to protected data objects*[43].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *surpassed*[44], the TSF shall *block access for that entity via the relevant interface to data requiring prior authentication until the time period shown in the Authentication Failure Handling Table has elapsed*[45].

[40] re-authenticate
[41] [assignment: *list of conditions under which re-authentication is required*]
[42] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]
[43] [assignment: *list of authentication events*]
[44] [selection: *met, surpassed*]
[45] [assignment: *list of actions*]

ID	Type of authentication	Allowed range of authentication failures	Blocked time period
(i)	*[assignment: type of authentication]*	*[assignment: range of acceptable values]*	*[assignment: time period]*

Table 2: Authentication Failure Handling Table

Application Note 22

The authentication covered by FIA_AFL.1 is the authentication required for access to data requiring prior authentication as defined in FIA_UAU.6. The types of authentication are therefore required to cover all types of data included in the Re-authentication Table.

Setting the allowed number of unsuccessful attempts and the time period during which access is blocked is specified in FMT_MOF.1.

6.3.4 Protection of the TSF

6.3.4.1 Failure with preservation of secure state (FPT_FLS.1)

FPT_FLS.1	*Failure with preservation of secure state*

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

(1) *Watchdog trigger results in meter reset*

(2) *Failure of the random bit generator*

(3) *[assignment: list of other types of failures and recovery actions in the TSF]*[46].

6.3.4.2 Tamper notification (FPT_TNN.1)

FPT_TNN.1	*Tamper notification*

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:

(1) Magnetic interference

[46] [assignment: *list of types of failures in the TSF*]

(2) [assignment: *list of additional physical tampering scenarios*].

Application Note 23

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, or the sending of a particular alarm message, or the recording of a particular log entry. The content of the alarm message and/or log entry should be described using FAU_ARP.2, 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.

Where an alarm is raised, this shall be sent at or before the meter's next default communication opportunity.

The final assignment for additional tampering scenarios may be left blank if no additional scenarios are supported.

The requirement to monitor and notify the presence of magnetic interference relates to the electromagnetic disturbances requirements of the EU Measuring Instruments Directive 014/32/EU.

6.3.4.3 Basic TSF Self Testing (FPT_BST.1)

FPT_BST.1	*Basic TSF Self Testing*

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), on reset]*[47] to demonstrate the correct operation of the TSF:

(1) *Firmware integrity test*

(2) *Random bit generator test*

(3) *Correct TSF start-up*

(4) *[assignment: list of additional self-tests run by the TSF on start-up]*[48].

Application Note 24

The ST author defines in the TOE Summary Specification the specific tests carried out.

6.3.4.4 Replay detection (FPT_RPL.1)

FPT_RPL.1	*Replay detection*

Dependencies: No dependencies

[47] [selection: *during initial start-up (on power on), periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self-tests should occur]*]

[48] [assignment: *list of self-tests run by the TSF*]

FPT_RPL.1.1	The TSF shall detect replay for the following **message types**[49]: [assignment: *list of identified message types*][50].
FPT_RPL.1.2	The TSF shall ~~**perform**~~ *[selection: discard the message, discard the message and [assignment: list of additional actions]]*[51] when replay is detected.

6.3.4.5 Reliable time stamps (FPT_STM.1)

FPT_STM.1	*Reliable time stamps*

Dependencies: No dependencies

FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.

Application Note 25

The TOE must provide timestamps suitable for supporting the time in an audit record for FAU_GEN.1.

6.3.4.6 Trusted update (FPT_TSU.1)

FPT_TSU.1	*Trusted Software/Firmware Update*

Dependencies: FCS_COP.1

FPT_TSU.1.1	The TSF shall provide [assignment: *list of authorised roles*] the ability to query [selection, one of: *the currently executing version of the TOE* ***firmware***[52], *the currently executing and the most recently downloaded versions of the TOE* ***firmware***[52]].
FPT_TSU.1.2	The TSF shall provide means to authenticate and verify the integrity of ***firmware***[52] updates to the TOE prior to installing those updates, using a digital signature mechanism that meets the following: [assignment*: mechanism specification*].
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*: list of additional properties*].
FPT_TSU.1.4	The TSF shall provide [assignment: *list of authorised roles*] the ability to activate updates to TOE ***firmware***[52].

Application Note 26

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.

In some cases the 'version' of the TOE firmware may be made up of a number of versions for individually identified components of that firmware.

---

[49] Refinement of "entities" consistent with section J.8 of [2].
[50] [assignment: *list of identified entities*]
[51] [assignment: list of specific actions]
[52] *software/firmware* – cf. the Glossary definition of firmware applicable in this Protection Profile

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 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.

As noted for O.SecureUpdate, FPT_TSU.1 applies to all firmware in the TOE that can be updated.

6.3.5 Security Management

6.3.5.1 Security roles (FMT_SMR.1)

FMT_SMR.1	*Security roles*

Dependencies:	FIA_UID.1 Timing of identification[53].
FMT_SMR.1.1	The TSF shall maintain the roles [assignment: *the authorised identified roles*].
FMT_SMR.1.2	The TSF shall be able to associate **received messages and keys**[54] with roles.

Application Note 27

Role-based access controls are defined in FDP_ACF.1, FDP_IFF.1/Msgs, FDP_IFF.1/Keys, FPT_TSU.1, FMT_MOF.1, FMT_MTD.1/Audit and FMT_MTD.1/Time.

The roles described here include all the roles necessary to use any type of access on any of the available interfaces in FDP_IFF.1/Int, which include all operational interfaces to the device. The list of roles thus includes any roles that have special access not available to other roles, such as administrative or maintenance roles.

If the permissions allocated to roles are configurable then this is described by the ST author in FMT_MOF.1.

6.3.5.2 Management of Security Functions Behaviour (FMT_MOF.1)

FMT_MOF.1	*Management of Security Functions Behaviour*

Dependencies:	FMT_SMR.1 Security roles
	FMT_SMF.1 Specification of Management Functions

[53] Note that this dependency is not required in this PP because of the refinement in FMT_SMR.1.2 – see section 7.2.2.

[54] The original word "users" is refined here because the TOE is expected to deduce a claimed role from a message and/or (in the case of any imported keys) from the method used to import a key; the roles in a smart meter infrastructure will be at the level of organisations (e.g. supplier or network operator) rather than individuals.

FMT_MOF.1.1 The TSF shall restrict the ability to *determine the behaviour of*[55] the functions *listed in the TSF Configuration Table*[56] to *the authorised identified roles in the TSF Configuration Table*[57].

Application Note 28

For each row in the TSF Configuration Table, if configuration of the identified item in the Function column is possible then the ST author selects 'Configurable' in the Configurable Status column for that row, and adds the list of roles that can configure it in the final column of the row. If it is not possible to configure this TSF data then the ST author selects 'Not configurable' in the Configurable Status column and completes the assignment in the final column of that row ('the authorised identified roles') as 'None'. The ST author may add other rows to the table below the rows specified in the PP, if applicable.

ID	Function	Configurable status	Roles Authorised for Configuration
(i)	*Allowed number of consecutive failed authentication attempts (FIA_AFL.1)*	*[selection, choose one of: Configurable, Not configurable]*	*[assignment: the authorised identified roles]*
(ii)	*Time period for blocking access after the allowed number of consecutive failed authentication attempts has been exceeded (FIA_AFL.1)*	*[selection, choose one of: Configurable, Not configurable]*	*[assignment: the authorised identified roles]*
(iii)	*Protection level applied to exchange of categories of application data (FDP_IFF.1/Msgs)*	*[selection, choose one of: Configurable, Not configurable]*	*[assignment: the authorised identified roles]*
(iv)	*Triggering of an alarm on the occurrence of an event (FAU_ARP.2)*	*[selection, choose one of: Configurable, Not configurable]*	*[assignment: the authorised identified roles]*
(v)	*Destination of an alarm on the occurrence of an event (FAU_ARP.2)*	*[selection, choose one of: Configurable, Not configurable]*	*[assignment: the authorised identified roles]*
(vi)	*Permissions allocated to roles (FDP_ACF.1, FDP_IFF.1/Msgs, FDP_IFF.1/Keys, FPT_TSU.1, FMT_MOF.1, FMT_MTD.1/Audit FMT_MTD.1/Time)*	*[selection, choose one of: Configurable, Not configurable]*	*[assignment: the authorised identified roles]*

Table 3: TSF Configuration Table

[55] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
[56] [assignment: *list of functions*]
[57] [assignment: *the authorised identified roles*]

Application Note 29

For row (iii), the ST author identifies any configuration that the TSF permits of the protection levels in terms of the message types and attributes identified in FDP_IFF.1/Msgs. This can be done by identifying each of the different available types of configuration when completing the assignment of 'authorised identified roles' (e.g. "…protection level for 'meter update' message type by Meter Owner role only; protection level for 'Energy Supplier update' messages by Supplier role only; …"). If permissions allocated to roles are configurable in row (vi) then the impact of this configurability must be noted by the ST author for any other SFRs that require identification of permitted roles (e.g. FMT_MOF.1, all FMT_MTD.1 iterations, and FAU_SAR.1). In other words: if permissions allocated to roles can change according to configuration settings, then the other SFRs that depend on permissions allocated to roles must be stated in a way that takes account of possible changes to the role-permissions configuration.

6.3.5.3 Management of TSF data (FMT_MTD.1) - Audit

FMT_MTD.1/Audit	*Management of TSF data*

Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/Audit	The TSF shall restrict the ability to *delete*[58] the *audit log records*[59] to [assignment: *the authorised identified roles*].

Application Note 30

When audit log records are overwritten because space for new records is exhausted (cf. FAU_STG.3 in section 6.3.6.6) then there may be no role involved and this situation does not need to be covered in this SFR. This SFR describes the roles that can delete (or clear) the audit log records for all other cases in which audit records are deleted. Any roles are taken from the list of defined roles in FMT_SMR.1 (section 6.3.5.1).

If an alarm message is sent before old records are overwritten then this is included under FAU_ARP.2 (Section 6.3.6.1).

6.3.5.4 Management of TSF data (FMT_MTD.1) - Time

FMT_MTD.1/Time	*Management of TSF data*

Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1/Time	The TSF shall restrict the ability to *modify*[60] the *meter time*[61] to [selection, choose one of: [assignment: *the authorised identified roles*].

[58] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[59] [assignment: *list of TSF data*]
[60] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[61] [assignment: *list of TSF data*]

6.3.6 Security Audit

6.3.6.1 Security Event Alarm (FAU_ARP.2)

FAU_ARP.2	*Security Event Alarm*

Dependencies: No dependencies

FAU_ARP.2.1 The TSF shall send an alarm message to the indicated destination for the following events:

- *Critical events: [assignment: list of events and destination for the alarm for each event]*
- *Physical tampering events: [assignment: list of events and destination for the alarm for each event]*
- *Other events: [assignment: list of events and destination for the alarm for each event]*[62].

FAU_ARP.2.2 The TSF shall include within each alarm message at least the following information:

a) Date and time of the event;
b) Type of event.

FAU_ARP.2.3 The TSF shall include the following additional alarm information: [assignment: *list of alarm messages and associated additional information*].

FAU_ARP.2.4 The TSF shall send alarms according to the following timing rules:

- *Alarms shall be sent at or before the meter's next default communication opportunity*[63].

Application Note 31

If the criteria for sending alarms are configurable in the TOE then this is specified in FAU_ARP.2.1 and the constraints on the roles that can perform configuration are specified in FMT_MOF.1. The physical tampering scenarios as specified in FPT_TNN.1 are included in the physical tampering events in FAU_ARP.2.1 – other events included in FPT_TNN.1 that result in sending of alarm messages should also be included in this SFR.

6.3.6.2 Audit data generation (FAU_GEN.1)

FAU_GEN.1	*Audit data generation*

Dependencies: FPT_STM.1 Reliable time stamps

[62] [assignment: *list of events and destination for the alarm for each event*]
[63] [assignment: *rules that specify when an alarm must be sent relative to the detection of the event*]

FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) ~~**Start-up and shutdown of the audit functions;**~~[64] b) ~~**All auditable events for the *not specified*[65] level of audit; and**~~[66] c) *Power-up/resume of the TOE* d) *Power-down of the TOE* e) *Reset or reboot of the TOE* f) *Reset triggered by watchdog timer (FPT_FLS.1)* g) *Change in network status* h) *Energy supply connect/disconnect* i) *Load limitation configuration/activation* j) *Authentication failure (FIA_UAU.6, FIA_AFL.1)* k) *Successful firmware update (FPT_TSU.1)* l) *Firmware update attempt failure due to invalid digital signature (FPT_TSU.1)* m) *Setting/updating meter time (FMT_MTD.1/Time)* n) *Tamper detection events (FPT_TNN.1)* o) *Detected replay events (FPT_RPL.1)* p) *Change of stored external party key (FDP_IFF.1/Keys)* q) *Key generation (FCS_CKM.1)* r) *Message received from an unauthorised source (FDP_IFF.1/Msgs)* s) *Key received from an unauthorised source (FDP_IFF.1/Keys)* t) *Change of stored meter key (FDP_IFF.1/Keys)* u) *Change of access rights (FAU_SAR.2, FMT_MOF.1)* v) *Device error events as follows: [assignment: list of auditable device error events] (FPT_BST.1, FPT_FLS.1)* w) *Failure of the random bit generator ((FPT_BST.1, FCS_RNG.1)* x) *Clearing the audit log (FAU_STG.1)* y) *Security anomaly events as follows: [assignment: list of auditable security anomaly events]* z) *Modification of [assignment: list of specified auditable data categories]* aa) *Self-test completed [FPT_BST.1]* bb) *[assignment: other specifically defined auditable events]*[67].
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information:

[64] In [2] FAU_GEN.1.1 includes a requirement to log start-up and shut-down of the audit functions. However, these are removed by refinement for the purposes of this PP because audit functions cannot be shut down in a smart meter.

[65] [selection, choose one of: *minimum, basic, detailed, not specified*]

[66] Levels of audit are not required to be defined in the Security Target, and therefore this is refinement removes the reference to a named level.

[67] [assignment: *other specifically defined auditable events*]

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST:
   - *Each audit record shall include a sequence number;*
   - *[assignment: other audit relevant information]*[68].

Application Note 32

If a listed event can never arise on a meter then the audit requirement for that event is considered to be trivially satisfied. For example, if the meter does not generate its own keys (cf. Application Note 10) then the requirement in item p) is considered to be trivially satisfied, although any change of the stored meter key (e.g. due to receiving an updated key from an authorised source) must be audited for item s).

The events 'message received from an unauthorised source' and 'key received from an unauthorised source' in FAU_GEN.1.1 items r) and s) are interpreted by the ST author according to the specific mechanisms used to receive messages and keys, as described for FDP_IFF.1/Msgs and FDP_IFF.1/Keys (e.g. this may be message-based or channel-based).

In some TOEs, FAU_GEN.1.1 item q) (meter key generation) and item t) (change of stored meter key) may be the same event, provided that the log record makes it unambiguous which key has been generated.

'Security anomaly events' in FAU_GEN.1.1 item y) are events that are logged in order to assist in detection or investigation of security incidents involving the TOE. The 'auditable data categories' in FAU_GEN.1.1 item z) are related to the objects defined in the access control rules in FDP_ACF.1.

6.3.6.3 Audit review (FAU_SAR.1 – refined)

FAU_SAR.1	*Audit review*
Dependencies:	FAU_GEN.1 Audit data generation
FAU_SAR.1.1	The TSF shall provide [assignment: *authorised users*] with the capability to read *the contents*[69] from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in **the format specific in the following reference: [assignment: *document reference details*]**[70].

Application Note 33

The method of authorisation for reading audit records is described in FAU_SAR.2 (section 6.3.6.4).

6.3.6.4 Restricted audit review (FAU_SAR.2 – refined)

FAU_SAR.2	*Restricted audit review*
Dependencies:	FAU_SAR.1 Audit data generation

[68] [assignment: *other audit relevant information*]
[69] [assignment: *list of audit information*]
[70] Refinement of "a manner suitable for the user to interpret the information" – the use of a documented definition of the format is considered to be suitable in the context of smart metering infrastructure.

FAU_SAR.2.1	The TSF shall prohibit all users read access to the audit records, except those users that have been granted ~~**explicit**~~ read-access **by [assignment: *description of method for assigning access*]**[71].

6.3.6.5 Protected audit trail storage (FAU_STG.1)

FAU_STG.1	*Protected audit trail storage*

Dependencies:	FAU_GEN.1 Audit data generation
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2	The TSF shall be able to *prevent*[72] ~~**unauthorised**~~[73] modifications to the stored audit records in the audit trail.

Application Note 34

Authorised deletion of audit log records is as specified in FMT_MTD.1/Audit (section 6.3.5.3) and is not considered to be a 'modification' of the log records. It is not expected that the TOE will allow any form of modification to stored audit records.

6.3.6.6 Action in case of possible audit data loss (FAU_STG.3)

FAU_STG.3	*Action in case of possible audit data loss*

Dependencies:	FAU_STG.1 Protected audit trail storage
FAU_STG.3.1	The TSF shall *overwrite the oldest record*[74] if the audit trail exceeds [assignment: *pre-defined limit* ***in terms of number of records supported***][75].

Application Note 35

If the TOE overwrites audit records when space for new records is exhausted then this SFR applies to the action taken before overwriting audit records that have not yet been read from the TOE.

6.4 Security Assurance Requirements

The evaluation assurance level for this PP is EAL3 augmented with ALC_FLR.3**.** The assurance components are identified in the table below (with augmentations in bold).

[71] This refinement text is added and replaces the original idea of explicit read access. In the context of smart metering infrastructure assignment of read-access might vary between schemes (and might be static or dynamic), but is always expected to have a well-defined description that can be used to complete the assignment.

[72] [selection, choose one of: *prevent, detect*]

[73] This refinement is intended to make clear that no modification of stored audit records is allowed (i.e. no roles are authorised to do this) – deletion of records is protected by authorisation as in FAU_STG.1.1.

[74] [assignment: *actions to be taken in case of possible audit storage failure*]

[75] [assignment: *pre-defined limit*]

Assurance Class	Assurance Components
Security Target (ASE)	ST introduction (ASE_INT.1)
	Conformance claims (ASE_CCL.1)
	Security problem definition (ASE_SPD.1)
	Security objectives (ASE_OBJ.2)
	Extended components definition (ASE_ECD.1)
	Derived security requirements (ASE_REQ.2)
	TOE summary specification (ASE_TSS.1)
Development (ADV)	Security architecture description (ADV_ARC.1)
	Functional specification with complete summary (ADV_FSP.3)
	Architectural design (ADV_TDS.2)
Guidance documents (AGD)	Operational user guidance (AGD_OPE.1)
	Preparative procedures (AGD_PRE.1)
Life cycle support (ALC)	Authorisation controls (ALC_CMC.3)
	Implementation representation CM coverage (ALC_CMS.3)
	Delivery procedures (ALC_DEL.1)
	Identification of security measures (ALC_DVS.1)
	Developer defined life-cycle model (ALC_LCD.1)
	Systematic flaw remediation (ALC_FLR.3)
Tests (ATE)	Functional testing (ATE_FUN.1)
	Analysis of coverage (ATE_COV.2)
	Testing: basic design (ATE_DPT.1)
	Independent testing – sample (ATE_IND.2)
Vulnerability assessment (AVA)	Vulnerability analysis (AVA_VAN.2)

Table 4: Security Assurance Requirements

6.4.1 Refinements of Security Assurance Requirements

The following refinements are made to selected assurance requirements in Table 4.

6.4.1.1 Derived Security Requirements (ASE_REQ.2)

ASE_REQ.2	*Derived security requirements*

Refinement:

When interpreting the generic work unit requirements for ASE_REQ.2 to apply to the meter, the evaluator shall check that the SFRs in the ST are consistent in their descriptions as described in the PP Application Notes (e.g. the action in the case of a meter that does not generate keys as described in Application Note 10, and the complete coverage of interfaces, operations and data between SFRs as described in Application Note 17).

6.4.1.2 Security Architecture Description (ADV_ARC.1)

ADV_ARC.1	*Security architecture description*

Refinement:

When interpreting the generic work unit requirements for ADV_ARC.1 to apply to the meter, the following specific topics must be addressed for this Protection Profile. It is acceptable for references to deliverables supplied for other assurance families, such as ADV_FSP, to be used to meet these requirements, provided that the relationship of the relevant interface specifications to the concepts in the Protection Profile is clear.

1. The Security Architecture Description shall include:
    a) A description of the parts of the TOE firmware that can be updated and the mechanisms used to perform the updates. The evaluator shall confirm that all parts of the TOE firmware that can be updated are updated according to FPT_TSU.1
    b) A description of the way in which the TOE erases keys (for FCS_CKM.4) and deallocates objects identified in FDP_RIP.1. This shall include source code excerpts and corresponding compiler output showing that the deletion process is effective, that it is retained during compilation (e.g. that it is not removed by compiler optimisation rules) and is applied at all necessary points in the TSF (i.e. in all situations where the keys and objects are deleted). The evaluator shall confirm that the code meets the requirements of the SFRs, and that it is applied in all relevant deletion situations.
2. The evaluator assessment of ADV_ARC.1.4C and ADV_ARC.1.5C shall include:
    a) Confirmation that the developer's lifecycle includes effective techniques to prevent and minimise the likely effects of failures, flaws or effects of malicious payloads sent to the meter. Examples of such techniques could be static analysis using MISRA rules, and use of compiler-supported stack protection. Note that use of these techniques is closely related to the requirement (in the refinement of ADV_TDS.2) for a rationale relating to the use of firmware protection measures.
    b) Confirmation that the access controls over types of data defined in FDP_ACF.1.1 are given equivalent protection when the data is accessed via messages, according to the rules in FDP_IFF.1/Msgs (possibly in combination with the rules in FDP_IFF.1/Keys)
    c) Confirmation that data exchanges between the meter and message originator/recipient are protected over the entire communication path between the endpoints.

6.4.1.3 Functional Specification with Complete Summary (ADV_FSP.3)

ADV_FSP.3	*Functional specification with complete summary*

Refinement:

When interpreting the generic work unit requirements for ADV_FSP.3 to apply to the meter, the following specific topics must be addressed for this Protection Profile. It is acceptable for references to deliverables supplied for other assurance families to be used to meet these requirements, provided that the relationship of the relevant interface specifications to the concepts in the Protection Profile is clear.

1. The Functional Specification shall describe, for each interface to the meter that is available and that is enabled, how the security requirements supporting the SFRs are implemented for messages at different levels of protocol (e.g. application and communications levels). The evaluator shall confirm that the application layer implements at least the following security properties for defined groups of messages[76]:
    - Authentication of message origin
    - Protection against replay of messages
    - Encryption of sensitive data
    - Integrity protection of message content
    - Authorisation rules to recognise sources that are permitted to send the message type.

    This may be demonstrated by reference to external reference documents (e.g. message specifications for a national smart meter infrastructure). Different groups of message types may be allocated different levels of protection, but the level of protection for each message type must be specified (such that the expected protection for any given message can be unambiguously determined from the specification). The description shall include the protocols used and the ways that the relevant security properties (authentication, encryption, etc.) are provided by cryptographic mechanisms.

    The Functional Specification shall identify any secure channels (or other secure communication mechanism) used for the import of secret or private keys or random bits (cf. Application Note 10, Application Note 17). The evaluator shall check that these secure channels are described in SFRs, and that they are included in the testing for ATE_IND.

2. The evaluator shall confirm that all message types, operations and data types available over all interfaces are covered unambiguously by the defined protection and authorisation rules in the Meter Data SFP (FDP_ACF.1), Messages SFP (FDP_IFF.1/Msgs), and the Keys SFP (FDP_IFF.1/Keys).
3. Description of the cryptographic mechanisms shall include:
    - Cryptographic algorithms
    - Key and signature length
    - Client/server authentication
    - Specification of entropy
    - Cryptographic Random Bit Generation

[76] This means that relevant protection, such as encryption, MAC or signature, must be applied in the application layer and must not rely only on lower level properties of the transmission channel or its protocol.

- Storage of keys.

The evaluator shall confirm that all cryptographic mechanisms and key management mechanisms used are defined in terms of open standards. The developer shall identify the source used for definition of approval of the mechanisms used by the meter, and the evaluator shall check that this information is included in the ST.

4. All keys required for the enforcement of the SFRs shall be listed in the design documentation, and for each key the following details shall be described:
    - purpose of the key
    - source (e.g. import or specific method of internal generation in the meter)
    - storage location (e.g. non-volatile memory within the meter, or a separate tamper-resistant secure module within the meter case)
    - storage format (e.g. wrapped according to a specified standard)
    - the method of replacement (if applicable) (e.g. in terms of a specific message type from a specific role)
    - the method of destruction of the key (cf. FCS_CKM.4).

    The evaluator shall check this list against the rules in FDP_IFF.1/Keys to ensure that all keys are covered by the defined rules.

5. The Functional Specification shall identify all interfaces to the meter that are available, and shall distinguish any of these interfaces that are disabled as required by FDP_IFC.1.5/Int from those interfaces that are enabled. The Functional Specification shall describe which functional interfaces are accessible over each of the communications interfaces (WAN, Neighbourhood Network, Local Network or direct connection). (Note that the refinement of ADV_TDS.2 requires additional information about these disabled interfaces.) The evaluator shall check that only operational interfaces are enabled in the operational configuration, and that these are all subject to the SFRs.
6. The Functional Specification shall specify any roles and associated interfaces that are supported in any stage of the device lifecycle (e.g. menus or command sets that are available before installation or after decommissioning). The device design information shall include a complete definition of the logical and physical interfaces that are available (such that the information could be used to create a test tool that will exercise all parts of the interface, with an ability to define expected results for any communication). The evaluator shall check that any such interfaces from lifecycle stages other than the normal operational stage (i.e. as used to monitor the supply to a consumer) that are not fully governed by the SFRs are not accessible in the normal operational stage.
7. The evaluator shall confirm, by examining the relevant channel, protocol and message definitions, that entities with which the meter communicates by messaging are uniquely identifiable.
8. The Functional Specification shall describe the types of failure identified by the TSF and the recovery actions taken by the TOE for FPT_FLS.1 (this information is used by the evaluator to support testing of failures as part of ATE_IND).
9. The Functional Specification shall describe the boundary over which FPT_TNN.1 applies in terms of the meter architecture (this information is used by the evaluator to support testing of physical protection in FPT_TNN.1 and FDP_IFF.1/Int as part of ATE_IND and AVA_VAN).

10. Description of the digital signature mechanism used for firmware updates (FPT_TSU.1), including the format of the updates. (This supports evaluator testing of specific types of unsuccessful update attempts as part of ATE_IND).

6.4.1.4 Architectural Design (ADV_TDS.2)

ADV_TDS.2	*Architectural design*

Refinement:

When interpreting the generic work unit requirements for ADV_TDS.3 to apply to the meter, the following specific topics must be addressed for this Protection Profile as part of the TOE Design Specification:

1. The TOE Design shall describe the mechanisms that protect data at rest in the meter. The evaluator shall confirm that these are sufficient to enforce the data protection SFRs in FDP_ACF.1 and FDP_IFF.1/Keys.
2. The TOE Design shall describe, in terms of the firmware design, why all operational interfaces are subject to the requirements of FDP_ACF.1, FDP_IFF.1/Msgs and FDP_IFF.1/Keys (e.g. in terms of the paths through which received messages are routed in the firmware and the order of processing fields in inputs).
3. The TOE Design shall justify that all instances of cryptographic mechanisms used at meter interfaces (e.g. for message protection, authentication, and random seed creation) and to protect data at rest (e.g. encryption of confidential information stored inside the meter) use approved mechanisms, and shall identify the nature of the approval and any relevant evidence (e.g. NIST CAVP certificates). The evaluator shall confirm the correctness of any identified evidence (i.e. that they relate to the relevant TOE components and that the components are used in accordance with any conditions of the certification)
4. The TOE Design shall describe the keys held in the meter, their source (e.g. imported, or generated in the meter using FCS_RNG.1), their storage location in the meter, and their storage format (e.g. wrapped or encrypted by a key encryption key). The evaluator shall confirm that this information is consistent with the requirements of FCS_CKM.1, FCS_CKM.4, and FDP_IFF.1/Keys
5. The TOE Design shall identify and describe the purpose of all data generated by the random bit generator in the TOE. (This information supports the evaluator analysis of key generation and support for any randomness properties relied upon in other SFRs.)
6. The TOE Design shall describe the way in which the boundary over which FPT_TNN.1 is enforced, at a level of detail that enables evaluators to construct and carry out tests to investigate the generation of the relevant notifications when the tamper events occur (FPT_TNN.1). (This information supports evaluator testing under ATE_IND and AVA_VAN.)
7. The TOE Design shall describe the purpose and use of any interface that is presented but disabled as required by FDP_IFF.1.5/Int (i.e. what is intended to be achieved by using the interface and the protocols/commands that it uses). In particular this description shall describe:
    - what elements of the TOE (e.g. configuration data, other stored data, firmware) are accessible over the interface before it is disabled
    - how the interface is disabled
    - whether the disabled state of the interface is reversible, and how any such re-enablement is achieved.

The evaluator shall confirm that the methods of disablement are of at least equivalent strength to the methods of authorisation for access to data and functions in the TOE, and that any re-enablement attack can only be carried out in physical proximity to the device and above the attack potential required under AVA_VAN.

8. The TOE Design shall include a rationale for how specific firmware protection measures are included in order to prevent or mitigate the potential effects of failures, flaws or malicious payloads sent to the meter. Examples of such techniques could be static analysis against MISRA rules, stack and heap protection measures to respond to corruption of these structures, and making it impossible to execute code from certain areas of memory. This rationale supports the evaluator analysis (in the refinement of ADV_ARC.1) to confirm the use of effective techniques to prevent and minimise the likely effects of failures, flaws or effects of malicious payloads.

6.4.1.5 Operational User Guidance (AGD_OPE.1)

AGD_OPE.1	*Operational user guidance*

Refinement:

When interpreting the generic work unit requirements for AGD_OPE.1 to apply to the meter, the following specific topics must be addressed for this Protection Profile as part of the Operational Guidance for the TOE:

1. Resources available for the audit log shall be described, including their limitations, such that users (i.e. the AMI system entities concerned with collecting and analysing the audit log) are made aware of any situations in which audit information might be lost (FAU_STG.3)
2. Resources available for firmware updates and any operational limitations imposed during the update process (FPT_TSU.1)
3. Description of the access control policies and identification of the implementation-specific objects that they refer to, including those objects referred to as ‘metrologically certified data’, ‘credentials’, ‘meter configuration’ and ‘controlled meter data items’ in FDP_ACC.2 and FDP_ACF.1.
4. Description of any user actions required in order to put the meter into its operational configuration (e.g. any configuration steps, key generation, or trust anchor key installation). The evaluator shall confirm that this is consistent with the description of keys in the TOE Design, and with the requirements of the SFRs.
5. Description of the results of self-tests carried out by the meter or secure failure recovery actions, and the expected actions from the user in response to each of these results (cf. FPT_BST.1, FPT_FLS.1)
6. Description of configurable parameters and their allowed values (cf. FMT_MOF.1). If the allowed actions for roles are configurable then this must also be described in the operational guidance.

6.4.1.6 Identification of Security Measures (ALC_DVS.1)

ALC_DVS.1	*Identification of Security Measures*

Refinement:

When interpreting the generic work unit requirements for ALC_DVS.1 to apply to the meter, the following specific topics must be addressed for this Protection Profile as part of the Development Security for the TOE:

1. The development security documentation shall include a description of the security-related activities carried out in the manufacturing environment of the meter and the security measures implemented to protect those activities. Examples of such activities would be disabling of test interfaces, installation of public key certificates to act as trust anchors, generation and injection of keys or random number seeds, and setting default security configuration parameters.
2. In addition to visiting the development environment, the evaluator shall also visit the manufacturing environment to examine the implementation of the security measures, to determine that the security measures are being applied, and to determine the sufficiency of the security measures employed.
3. The evaluator shall confirm that manufacturing leaves the meter in a secure state in which unauthorised users cannot change the security configuration (e.g. by changing access controls or changing installed keys), or else that the delivery procedures sufficiently protect the physical instances of the TOE against tampering between manufacturing and delivery to the customer.

6.4.1.7 Independent Testing – Sample (ATE_IND.2)

ATE_IND.2	*Independent testing – sample*

Refinement:

When interpreting the generic work unit requirements for ATE_IND.2 to apply to the meter, for the purposes of this Protection Profile the evaluator's test sample shall include at least:

1. Testing the correct response to consecutive authentication failures that exceed the threshold in FIA_AFL.1 as configured according to FMT_MOF.1 (in terms of the failures threshold and the time for which access is blocked)
2. Testing that re-authentication behaviour is as specified (FIA_UAU.6).
3. Testing each of the rules for message protection in FDP_IFF.1/Msgs. As part of the tests the evaluator shall check that the cryptographic formatting specified in design deliverables is applied to messages sent to the TOE (e.g. by constructing messages in accordance with the design deliverables) and responses received from the TOE (e.g. by decoding responses, including decrypting and checking MACs and signatures as specified in the design deliverables).
4. Testing each of the rules for export of meter keys in FDP_IFF.1/Keys
5. Testing each of the rules for import of other entity keys in FDP_IFF.1/Keys
6. Testing communications failures of the following types:
    - message floods
    - out-of-sequence messages
    - malformed messages
    - lack of expected response
    - lack of expected regular input.
7. Testing for correct rejection of a sample of replayed messages (FPT_RPL.1).
8. Testing a sample of the failure types identified in FPT_FLS.1.

9. Testing a sample of the failure types identified in FPT_BST.1.
10. Testing a sample of the tampering events identified in FPT_TNN.1 and.
11. Testing successful firmware update and unsuccessful update due to invalid digital signature conditions as in FPT_TSU.1 (depending on the signature mechanism this may require several tests to cover different reasons for failure, such as failure of a certification path validation, incorrect digital signature value, and incorrect image hash value (if the image hash is separate from the digital signature).
12. Confirming by examination of configuration interfaces that all the restriction of configuration operations is as specified in FMT_MOF.1, FMT_MTD.1/Audit and FMT_MTD.1/Time. This shall include a check that the relevant parameters either are not configurable or else can only be modified by the identified roles
13. If the TOE supports configuration of permissions allocated to roles (see row (vi) in the TSF Configuration Table and FMT_MOF.1) then this configuration shall also be tested in terms of both positive and negative effects (i.e. tests of changes to both actions allowed and actions not allowed).
14. The evaluator shall test the deletion of keys (as in FCS_CKM.4) and the objects identified in FDP_RIP.1, to demonstrate that after deletion then the key/object cannot be accessed via at least one of the functions that would previously have been used to access it.
15. The evaluator shall test at least one instance of each type of audit message in FAU_GEN.1.
16. The evaluator shall confirm by testing that unauthorised attempts to access the audit log are rejected (FAU_STG.1, FMT_MTD.1/Audit).

Note that testing of rules (such as in item 3 above) generally requires tests to demonstrate both positive (acceptance) and negative (rejection) cases.

6.4.1.8 Vulnerability Analysis (AVA_VAN.2)

AVA_VAN.2 *Vulnerability analysis*

When interpreting the generic work unit requirements for AVA_VAN.2 to apply to the meter, the evaluator shall address the following specific topics for this Protection Profile.

1. Confirming (including testing) that, after installation, the power-up process does not allow the device to be launched into any mode other than the normal operating mode (e.g. no access is granted to diagnostic or recovery functions, including engineering menus, other than those permitted via the enabled interfaces according to FDP_IFF.1/Int)
2. Confirming (including testing) that, cycling power preserves the blocking time in FIA_AFL.1.2 (i.e. cycling power does not provide a method to remove the block on access)
3. Confirming (including testing) that disabled interfaces as in FDP_IFF.1/Int are not usable in practice (using the information on the disabled interfaces provided in ADV_FSP.3 and ADV_TDS.2)

7 Rationales

7.1 Security Objectives Rationale

7.1.1 Security Objectives Coverage

The table below shows the mapping of Threats, Organisational Security Policies and Assumptions to Security Objectives for the TOE and for the TOE Environment.

	O.Authorisation	O.Messages	O.DataAtRest	O.Crypto	O.Interfaces	O.Resilience	O.SecureUpdate	O.Logging	O.Alarms		OE.ExternalData	OE.AuditSupport	OE.InspectionSupport	OE.UniqueSubjectIDs
T.NetworkDisclosure	X	X	X	X	X									
T. DirectDisclosure	X	X	X	X	X								X	
T.NetworkDataMod	X	X	X	X	X									
T. DirectDataMod	X	X	X	X	X								X	
T.Malfunction					X	X	X							
P.Logging								X						
P.Alarms									X					
A.ExternalData											X			
A.AuditSupport												X		
A.InspectionSupport													X	
A.UniqueSubjectIDs														X

Table 5: Security Problem Definition mapping to Security Objectives

7.1.2 Security Objectives Sufficiency

The following paragraphs describe the rationale for the sufficiency of the Security Objectives relative to the Threats, OSPs and Assumptions.

7.1.2.1 Threats

T.NetworkDisclosure is addressed by TOE objectives as follows:

- O.Authorisation requires that successful authorisation has been checked by the TOE before an action (such as reading) is carried out on data at the request of any direct or network entity
- O.Messages requires that messages are protected against various forms of attack that might otherwise enable unauthorised messages to be used to read data remotely
- O.DataAtRest requires that data stored in the TOE is protected against unauthorised access
- O.Crypto requires the use of approved cryptographic techniques which therefore provide suitable cryptographic strength to resist attackers
- O.Interfaces ensures that there are no interfaces available that would circumvent the protections above.

T.DirectDisclosure is addressed by TOE objectives as described for T.NetworkDisclosure above, noting that the relevant TOE Objectives apply to both direct and network entities. In addition, OE.InspectionSupport supports detection of attacks that rely on physical modification of direct interfaces.

T.NetworkDataMod is addressed by TOE objectives as described for T.NetworkDisclosure above, noting that the relevant TOE Objectives apply to data modification as well as to reading data.

T.DirectDataMod is addressed by TOE objectives as described for T. NetworkDisclosure above, noting that the relevant TOE Objectives apply to both direct and network entities and to data modification as well as to reading data. In addition, OE.InspectionSupport supports detection of attacks that rely on physical modification of direct interfaces.

T.Malfunction is addressed by TOE objectives as follows:

- O.Interfaces ensures that there are no interfaces available that might enable unauthorised access to induce faults or that might assist in exploiting security vulnerabilities arising from a malfunction
- O.Resilience requires that the TOE checks its start-up process, and detects and recovers from identified failures in a secure way[77].
- O.SecureUpdate ensures that the TOE provides a secure way to update its firmware, so that malfunctions can potentially be addressed by new firmware, but that the ability to load new firmware does not provide an opportunity for unauthorised modifications of the firmware.

7.1.2.2 Organisational Security Policies

P.Logging is addressed by O.Logging, which directly translates the policy into an objective for the TOE.

P.Alarms is addressed by O.Alarms, which directly translates the policy into an objective for the TOE.

[77] Of course it is not feasible to specify all possible failure cases, nor therefore to require that the TOE will recover a secure state in all cases. However, the identified failures are expected to address the highest risk cases that are foreseeable.

7.1.2.3 Assumptions

Each of the Assumptions in section 3.5 is directly matched by a security objective for the operational environment in section 4.2. The wording of each objective for the operational environment includes the wording of each assumption, and no further rationale is therefore given here.

7.2 Security Requirements Rationale

7.2.1 Security Requirements Coverage

The table below summarises the mapping of Security Objectives for the TOE to SFRs.

	O.Authorisation	O.Messages	O.DataAtRest	O.Crypto	O.Interfaces	O.Resilience	O.SecureUpdate	O.Logging	O.Alarms
FCS_CKM.1		X		X					
FCS_CKM.4		X	X						
FCS_COP.1		X		X			X		
FCS_RNG.1				X					
FDP_ACC.2	X		X						
FDP_ACF.1	X		X						
FDP_IFC.1/Msgs	X	X							
FDP_IFF.1/Msgs	X	X							
FDP_IFC.2/Int					X				
FDP_IFF.1/Int					X				
FDP_IFC.1/Keys	X			X					
FDP_IFF.1/Keys	X			X					
FDP_RIP.1			X						
FIA_UAU.6	X								
FIA_AFL.1	X								
FPT_BST.1						X			
FPT_FLS.1						X			
FPT_TNN.1								X	X
FPT_RPL.1		X							
FPT_STM.1								X	X
FPT_TSU.1							X		

	O.Authorisation	O.Messages	O.DataAtRest	O.Crypto	O.Interfaces	O.Resilience	O.SecureUpdate	O.Logging	O.Alarms
FMT_SMR.1	X							X	X
FMT_MOF.1	X								X
FMT_MTD.1/Audit								X	
FMT_MTD.1/Time	X							X	X
FAU_ARP.2									X
FAU_GEN.1								X	
FAU_SAR.1								X	
FAU_SAR.2								X	
FAU_STG.1								X	
FAU_STG.3								X	

Table 6: TOE Security Objectives mapping to SFRs

O.Authorisation is addressed by the TOE security requirements as follows:

- FDP_IFC.1/Msgs and FDP_IFF.1/Msgs state rules for authorisation of messages received by the TOE
- FDP_IFC.1/Keys and FDP_IFF.1/Keys state rules for authorisation specifically related to operations on keys (noting that keys will generally form the basis for the TOE to determine the authorisation of other messages)
- FIA_UAU.6 states requirements for authentication which forms the basis for authorisation (including both initial authentication and subsequent re-authentication after a defined expiry time for the initial authentication), with FIA_AFL.1 stating the requirements for acting on repeated authentication failures, and FMT_MOF.1 stating the requirements for defined authorisation parameters (including protection levels for categories of application data) and the roles that are permitted to set them
- FMT_MTD.1/Time ensures that only authorised roles can modify the TSF time (on which authorisation decisions and expiry of authentication) may be based
- FMT_SMR.1 supports the configuration permissions in FMT_MOF.1 and FMT_MTD.1/Time by defining the relevant roles.

O.Messages is addressed by the TOE security requirements as follows:

- FCS_CKM.1 and FCS_COP.1 describe the key generation and cryptographic operations that are used to support message protection; FCS_CKM.4 ensures the protection of the cryptographic keys from unauthorised access after of deletion

- FDP_IFC.1/Msgs and FDP_IFF.1/Msgs state rules for authorisation of messages received by the TOE, with respect to roles defined in FMT_SMR.1 (thus supporting protection against unauthorised disclosure/modification and against forgery) and ensure that the TOE will not respond to unauthorised messages
- FPT_RPL.1 requires specific protection against replay of identified message types (which may include all messages)
- Implementation of the protection at the application layer (therefore providing independence from the underlying communication protocol) is confirmed as part of the refinement of ADV_FSP.3 in section 6.4.1.3.

O.DataAtRest is addressed by the TOE security requirements as follows:

- FDP_ACC.2 and FDP_ACF.1 state the rules for authorised access to various types of data object
- FCS_CKM.4 and FDP_RIP.1 ensure that when keys and other data objects are deleted then they do not present opportunities for unauthorised access.

O.Crypto is addressed by the TOE security requirements as follows:

- FCS_CKM.1 and FCS_COP.1 describe the key generation and cryptographic operations used by the TSF protection mechanisms, and the standards that these are based on
- FCS_RNG.1 states the requirements on the random bit generator
- FDP_IFC.1/Keys and FDP_IFF.1/Keys state rules to control access to keys, thus supporting the security of the cryptographic mechanisms.

O.Interfaces is addressed by the TOE security requirements as follows:

- FDP_IFC.2/Int and FDP_IFF.1/Int state rules to control the availability of interfaces, identifying the interfaces required for normal operation and requiring all other interfaces to be disabled. The use of FDP_IFC.2 in this case emphasises the need for an ST to account for all the interfaces present in the TOE, regardless of their intended use
- Refinements of ADV_FSP.3 and ADV_TDS.2 support the identification with more detail that enables the evaluators to confirm the completeness of the interfaces identified, and require the strength of the disabling method to be consistent with the strength of protection provided for authentication and authorisation for other operations using message-based interfaces.

O.Resilience is addressed by the TOE security requirements as follows:

- FPT_BST.1 states requirements for self-test to ensure a secure start-up of the TOE
- FPT_FLS.1 states requirements for recovery to a secure state after defined failure conditions occur.

O.SecureUpdate is addressed by the TOE security requirements as follows:

- FPT_TSU.1 requires that the TSF provides a secure update mechanism based on digital signatures
- Refinement of ADV_ARC.1 includes a requirement for the evaluator to confirm that the secure mechanism applies to all TSF firmware that can be updated

- FCS_COP.1 specifies the cryptographic operation(s) used to protect authenticity and integrity of updates.

O.Logging is addressed by the TOE security requirements as follows:

- FPT_TNN.1 identifies requirements for physical tampering attempts to be logged
- FAU_GEN.1 states requirements for other events to be logged and the basic content of the log records
- FPT_STM.1 requires the TOE to provide accurate time for use in the log records, and FMT_MTD.1/Time ensures that this can only be modified by authorised roles
- FMT_MTD.1/Audit and FAU_STG.1 ensure that audit records can only be deleted by authorised roles and that they cannot be modified (by any role)
- FAU_SAR.1 requires that only authorised entities can read the audit log; this is reinforced by FAU_SAR.2 which requires the description of the specific method by which access is granted to the audit log
- FAU_STG.3 states the action to be taken if the log is in danger of filling up
- FMT_SMR.1 defines the roles on which audit activity and constraints are based.

O.Alarms is addressed by the TOE security requirements as follows:

- FAU_ARP.2 identifies the events that give rise to alarms (including the physical tamper and any other events required to raise alarms in FPT_TNN.1), and the basic content of an alarm
- FPT_STM.1 requires the TOE to provide accurate time for use in the log records, and FMT_MTD.1/Time ensures that this can only be modified by authorised roles
- FMT_MOF.1 defines the authorised roles that can configure alarm behaviour
- FMT_SMR.1 defines the roles on which alarm activity and constraints are based.

7.2.2 SFR Dependencies

The dependencies between SFRs are addressed as shown in Table 7. Where a dependency is not met in the manner defined in [2] then a rationale is provided for why the dependency is unnecessary or else met in some other way.

Requirement	**Dependencies**	**Fulfilled by**
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	FCS_COP.1 FCS_CKM.4 See also note below on distribution of keys generated in the meter

Requirement	Dependencies	Fulfilled by
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1 (for internally generated keys) See also note below on destruction of keys imported to the meter.
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	FCS_CKM.1 (for internally generated keys) See also note below on import of keys to the meter. FCS_CKM.4
FCS_RNG.1	No dependencies	
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.2 Because the attributes used for the access control rules are simply identity and/or role, no additional statement of management of these attributes in FMT_MSA.3 is considered necessary.
FDP_IFC.1/Msgs	FDP_IFF.1	FDP_IFF.1/Msgs
FDP_IFF.1/Msgs	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1/Msgs Because specific attributes for the SFP are not defined in the PP, the dependency on FMT_MSA.3 is not required.
FDP_IFC.2/Int	FDP_IFF.1	FDP_IFF.1/Int
FDP_IFF.1/Int	FDP_IFC.1 FMT_MSA.3	FDP_IFC.2/Int Because specific attributes for the SFP are not defined in the PP, the dependency on FMT_MSA.3 is not required.
FDP_IFC.1/Keys	FDP_IFF.1	FDP_IFF.1/Keys

Requirement	Dependencies	Fulfilled by
FDP_IFF.1/Keys	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1/Keys Because specific attributes are not defined in the PP, the dependency on FMT_MSA.3 is not required.
FDP_RIP.1	No dependencies	
FIA_UAU.6	No dependencies	
FIA_AFL.1	FIA_UAU.1	For this TOE the authentication conditions (and timing of authentication) for access to private data via the user interface are defined in FIA_UAU.6 (and the transitive dependency from FIA_UAU.1 to FIA_UID.1 is not applicable because users at the user interface are not individually identified).
FPT_BST.1	No dependencies	(Note that the completion of self-test is not required to be logged in this Protection Profile, but start-up and reset events and failures detected by the self-test are required to be logged – see FAU_GEN.1).
FPT_FLS.1	No dependencies	
FPT_TNN.1	No dependencies	
FPT_RPL.1	No dependencies	
FPT_STM.1	No dependencies	
FPT_TSU.1	FCS_COP.1	FCS_COP.1 Application Note 12 identifies the need for at least one separate iteration of FCS_COP.1 to specify the operations used for trusted updates.
FMT_SMR.1	FIA_UID.1	This dependency is not required because the TOE associates *messages* with roles, rather than *users* with roles. This approach reflects the organisational infrastructure used in smart metering.

Requirement	Dependencies	Fulfilled by
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 See also note below on identification of management functions.
FMT_MTD.1/Audit	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 See also note below on identification of management functions.
FMT_MTD.1/Time	FMT_SMR.1 FMT_SMF.1	FMT_SMR.1 See also note below on identification of management functions.
FAU_ARP.2	No dependencies	
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.1

Table 7 – SFR Dependencies Rationale

Distribution of keys generated in the meter: no particular method or rules are defined in this PP for distributing keys generated in a smart meter (cf. FCS_CKM.2 in [2]), because this distribution is expected to be specific to the particular AMI in which the meter is deployed and not susceptible to generic specification at the level of this PP.

Import of keys to the meter: no particular methods are assumed in this PP for import of secret, private or public keys from an external entity to the meter. However, if any keys are imported then any applicable rules for their import are stated in the ST in FDP_IFF.1/Keys in section 6.3.2.8.

Destruction of keys imported to the meter: although no specific import of keys is assumed in this PP, FCS_CKM.4 is applied to any imported secret or private keys as described in Application Note 11 (as well as to internally generated keys of course).

Identification of management functions: as all management operations are already identified in FMT_MOF.1 and FMT_MTD.1 iterations, the dependency on FMT_SMF.1 adds no additional information and is not required.

7.2.3 Rationale for SARs

The assurance level for this protection profile is EAL3 augmented with ALC_FLR.3.

EAL3 represents an assurance level based on the use of positive security engineering at the design stage, but that is consistent with good commercial practice. As such, EAL3 is appropriate to a metering environment demanding moderate security functions, and where some of the security contribution is made by the design of the cryptographic architecture and other AMI components. This is consistent with the description of EAL3 in [3] as “a moderate level of independently assured security, [requiring] a thorough investigation of the TOE and its development without substantial re-engineering”. Augmentation with ALC_FLR.3 is included as a recognition of the importance of timely remediation of any flaws discovered in meters after delivery and deployment.

8 References

[1] Common Criteria for Information Technology Security Evaluation,
Part 1: Introduction and General Model,
CCMB-2017-04-001, Version 3.1 Revision 5, April 2017

[2] Common Criteria for Information Technology Security Evaluation,
Part 2: Security Functional Components,
CCMB-2017-04-002, Version 3.1 Revision 5, April 2017

[3] Common Criteria for Information Technology Security Evaluation,
Part 3: Security Assurance Components,
CCMB-2017-04-003, Version 3.1 Revision 5, April 2017

Note that references [1], [2] and [3] above are also published as ISO/IEC 15408.

[4] Common Methodology for Information Technology Security Evaluation,
Evaluation methodology,
CCMB-2017-04-004, Version 3.1 Revision 5, April 2017

Note that reference [4] above is also published as ISO/IEC 18045.

[5] Smart Meter Co-ordination Group Privacy and Security Approach – Part IV: Minimum security requirements for AMI components – European level requirements for Smart Metering, v1.1, 17 July 2016

[6] Functional reference architecture for communications in smart metering systems, CEN/CLC/ETSI TR 50571, December 2011

Appendix A – Mapping to Minimum Security Requirements

This appendix gives tables that map the relevant requirements extracted from [5] to the SFRs, SARs and SAR refinements made in this Protection Profile. The first table maps the functionality-related requirements from [5], the second table maps the assurance-related requirements.

The requirements from [5] are marked with the following abbreviations to indicate the part of each requirement in which they are specified:

(Req)	Requirement
(SubReq)	Sub-requirement
(IG)	Implementation guideline
(AG)	Assurance guideline.

Minimum Security Requirement	Objective/SFR/SAR
A: All AMI components SHALL provide a log of security events	O.Logging O.Alarms
Include [5] Annex A events in audit log contents (Req)	FAU_GEN.1
register communication sessions and identify the users (IG)	FAU_GEN.1
register attempts to compromise the security of the device (IG)	FPT_TNN.1
provide alarm functionality for specific events (IG)	FAU_ARP.2
make the log accessible for evaluation via a standardized interface (IG)	FAU_SAR.1
Secure access to the log (SubReq)	FAU_SAR.2
Provide memory for a minimum number of entries. Mechanisms shall exist in order to prevent filling up the (FIFO) logs – The resources available for the log are documented (SubReq)	FAU_STG.3 AGD_OPE.1
Every entry SHALL have a timestamp and a sequence number (SubReq)	FAU_GEN.1 FPT_STM.1
Every entry SHALL identify the source of the security event (SubReq) – E.g. for tampering identify the nature of the event (broken seal, magnetic interference, etc.) (IG)	FAU_GEN.1
Critical events SHALL trigger alarms (SubReq) – The criterion for a critical event is defined and configurable (IG)	FAU_ARP.2
Each log entry SHALL be protected against modification (SubReq) – Role based access control is implemented only for clearing the log (resulting in a new event) (IG)	FAU_STG.1 FMT_SMF.1 FMT_SMR.1 FMT_MTD.1/Audit FAU_GEN.1
B: All data exchanges SHALL take place in a (end-to-end) secure manner	O.Messages
Protection against Replay, Disclosure, Modification, Impersonation during data exchange (e.g. readings, commands, alarms, credentials, etc.) (Req)	FPT_RPL.1 FDP_IFC.1/Msgs FDP_IFF.1/Msgs
All data exchanges SHALL be cryptographically protected and optionally also physically protected.	FCS_COP.1 FCS_CKM.1

Minimum Security Requirement	Objective/SFR/SAR
Since Risk Analysis may indicate different levels of protection are appropriate, exceptions to this encryption requirement MAY be possible for certain data e.g. the meter serial number (SubReq)	FCS_CKM.4
encryption (and authentication) is possible for messages exchanged between any AMI system component independent of the communication medium used for the data exchange (IG)	ADV_FSP.3
The manufacturer adds an incrementing counter per message to assist in detecting message replay or implements another replay protection such as a time based mechanism (e.g. token) (IG)	FPT_RPL.1
The protocols used for the message exchange are based on open standards (IG)	FCS_COP.1
Different levels of protection MAY be provided, depending on the type of the data (SubReq)	FMT__MOF.1 ADV_FSP.3
Data is classified into pre-defined application categories. The protection level is made configurable depending on the application category of the data (IG)	FMT__MOF.1 ADV_FSP.3
Security SHALL be implemented independently of the communication protocol. (SubReq)	ADV_FSP.3
Application layer security is implemented. In addition, lower layer security mechanisms may be implemented. (IG)	ADV_FSP.3
The contextual validity of information exchanged SHALL be checked. (SubReq)	FDP_IFF.1/Msgs
Validation of messages on system or on device level (where the context is available) is considered and the validation rules specified. For example the grid or credit status can be used as a context when activating the switch in a meter (IG)	FDP_IFF.1/Msgs
C: Availability of the system (AMI components and communication network) SHALL be sufficient to perform the Use Cases the system has been designed for	O.Resilience
The AMI system requirements describe the Use Cases to be supported by the system. The Smart Meters Coordination Group has developed a general set of AMI Use Cases (Req)	None
The manufacturers of the components provide standardized failure statistics, MTBF (mean time between failures) or others (IG)	None
The availability of the system SHALL be monitored (SubReq)	FAU_GEN.1
Supervision of the availability of the AMI components and the communication network is implemented. The communication network operator provides statistics on the reliability of the message exchange in the network. (IG)	FAU_GEN.1
The system and its components SHALL start-up and recover from failures in a defined and secure way (SubReq)	FPT_BST.1 FPT_FLS.1
The manufacturer implements and documents error recovery capabilities for the system and its components (IG)	FPT_BST.1 FPT_FLS.1

Minimum Security Requirement	Objective/SFR/SAR
The system SHALL be designed in such a way that if communication failures occur they have only minimal impacts on the system availability (SubReq)	None
In case of failure, system components SHOULD not compromise their own security or that of other components of the AMI (SubReq)	FPT_BST.1 FPT_FLS.1
D: Crypto mechanism and key management SHALL be documented and be compliant with recognized/proven and approved open standards	O.Crypto
The description of the crypto mechanisms and of the key management SHALL be publically available (based on open standards). (SubReq)	FCS_CKM.1 FCS_COP.1 FDP_IFC.1/Keys FDP_IFF.1/Keys ADV_FSP.3
Documentation SHALL include all implemented features, in particular: … - Cryptographic Random Number Generation … (SubReq) [Note that this confirms the requirement for implementation of a Random Number Generator)	FCS_RNG.1
E: Every AMI component SHALL check the authorisation of any entity requesting access to it and grant or deny access based on the result of that check	O.Authorisation
Entities include persons and components. Components are all system parts that support AMI functions. Authorisation determines the access rights of the entity to the AMI component (Req)	FDP_IFC.1/Msgs FDP_IFF.1/Msgs FDP_IFC.1/Keys FDP_IFF.1/Keys
Every data point and function SHALL have defined access rights (SubReq)	FDP_IFF.1/Msgs FDP_IFF.1/Keys
Every entity SHALL be uniquely identifiable (SubReq)	OE.UniqueSubjectIDs
Access SHALL be temporarily denied after a specified number of unsuccessful attempts (SubReq)	FIA_AFL.1
The time for denial of access and the number of unsuccessful attempts to trigger the denial is defined and configurable (IG)	FMT_SMF.1 FMT_MOF.1 ATE_IND.2
Access rights SHALL expire after a pre-defined time (SubReq)	FIA_UAU.6
The expiry time is defined and made configurable (IG)	FIA_UAU.6 FMT_MOF.1
F: Data at rest SHALL be protected in all system components	O.DataAtRest
Different levels of protection SHALL be provided, depending on the application category of the data. Categories include:	FDP_ACC.2 FDP_ACF.1

Minimum Security Requirement	Objective/SFR/SAR
- Metrologically certified data (e.g. consumption/generation measurements) - Credentials - Configuration - Firmware (SubReq)	
The system components implement different levels of protection in a documented way. All data that has been classified as sensitive (determined via the Risk Analysis) should have highest level of protection (IG)	FDP_ACC.2 FDP_ACF.1
Obsolete data SHALL be permanently deleted (SubReq)	FDP_RIP.1 FCS_CKM.4
A deletion function is implemented (IG)	ATE_IND.2 ADV_ARC.1
Modifications of data in specific application categories SHALL be identified and logged, including initiator details. (SubReq)	FAU_GEN.1
Implement a log file for modification of specific data categories (IG)	FAU_GEN.1
G: AMI components SHALL be upgradable to incorporate new (security) functionalities	O.SecureUpdate
This refers to both hardware and software (Req) [Note that this PP covers only updates to firmware/software]	FPT_TSU.1
Security functionality in AMI components SHALL be updatable (bug fixes) and upgradable (additional functionalities) (SubReq)	FPT_TSU.1
AMI components SHALL allow spare capacity (memory and CPU power) for updates and upgrades. (SubReq)	FPT_TSU.1
Integrity and authenticity of update images SHALL be verified before they are applied or activated. (SubReq)	FPT_TSU.1 FCS_COP.1
H: Functionalities in AMI components SHOULD be limited to the intended operational Use Cases and SHALL not be able to compromise security functions	O.Interfaces
Interfaces that are not used SHALL be disabled. (SubReq)	FDP_IFC.2/Int FDP_IFF.1/Int ADV_FSP.3 ADV_TDS.2 AVA_VAN.2
Disabled functions of AMI components SHALL not compromise security functions. (SubReq)	ADV_FSP.3 ADV_TDS.2
The system is designed in such a way that functionality blocks do not interfere with security functions in an unintended way (IG)	ADV_TDS.2
I: AMI components and the communications network SHALL be adequately protected against external disturbances and/or attacks and SHALL demonstrate resilience against attacks	O.Resilience

Minimum Security Requirement	Objective/SFR/SAR
Disturbances and attacks can be: tampering, EMC, Clock/ Date/ Time change, Denial of Service. (Req)	FPT_BST.1 FPT_FLS.1 FPT_TNN.1 FMT_MTD.1/Time
The manufacturer implements protection measures against a sufficient range of attacks, including: - Tampering - EMC - Clock/ Date/ Time - Denial of service (IG)	FPT_BST.1 FPT_FLS.1 FPT_TNN.1 FMT_MTD.1/Time

Table 8 - Minimum Requirements – Functional Requirements Mapping

Minimum Security Requirement	SAR/EAL note
A: All AMI components SHALL provide a log of security events	
The manufacturer provides design evidence ensuring that this requirement [that the is equipped with sufficient capabilities to do audit] is addressed. Design evidence is at a level of detail that enables easy verification (IG)	ADV_FSP.3 ADV_TDS.2 The general Assurance Guidance at Requirement level says “A minimal set of security compromising actions is applied to the component and the corresponding registration and alarms are checked” and is covered by the more detailed requirements below.
The resources available for the log are documented… (IG) The evaluator checks the documentation (AG)	Refinement of AGD_OPE.1
The evaluator checks the access control [to the log] by performing authorised and unauthorised access (AG)	Implicit in testing FAU_SAR.2, FAU_STG.1 + refinement of ATE_IND.2
The evaluator checks the log [for timestamp and serial number] (AG)	Implicit in testing FAU_GEN.1, FPT_STM.1
The evaluator checks the log [for source of event] (AG)	Implicit in testing FAU_GEN.1, FAU_SAR.2
The evaluator checks the alarms for specific events (AG)	Implicit in testing FAU_ARP.2
The evaluator checks the access control [protecting the log against modification] by performing authorised and unauthorised access (AG)	Implicit in testing FAU_SAR.2, FAU_STG.1 + refinement of ATE_IND.2

Minimum Security Requirement	SAR/EAL note
B: All data exchanges SHALL take place in a (end-to-end) secure manner	
The manufacturer provides design evidence ensuring that this requirement [to protect against replay, disclosure, modification, impersonation] is addressed. Design evidence is at a level of detail that enables easy verification. (IG)	Implicit in testing of FPT_RPL.1, FDP_IFC.1/Msgs, FDP_IFF.1/Msgs + refinement of ADV_ARC.1, ADV_FSP.3, ADV_TDS.2
AMI components are tested by sending correctly protected messages and incorrectly protected messages to the components. The responses of the AMI components are checked for correct protection. (AG)	Implicit in testing of FPT_RPL.1, FDP_IFC.1/Msgs, FDP_IFF.1/Msgs + refinement of ATE_IND.2
The manufacturer documents the security mechanisms and the protocols used in the AMI system… (IG) The evaluator checks the documentation for the security mechanisms used (AG)	Refinement of ADV_ARC.1, ADV_FSP.3, ADV_TDS.2, AGD_OPE.1
The evaluator checks that replayed messages are detected and rejected (AG)	Implicit in testing of FPT_RPL.1 + refinement of ATE_IND.2
Encryption and authentication is accessible for evaluation via a standardized interface. The protocols used for the message exchange are based on open standards… (IG) The evaluator confirms that the AMI component has been certified for implementing a standard protocol (AG)	Refinement of ADV_FSP.3 and ADV_TDS.2
Implement application layer security. Lower layer security mechanisms may be implemented… (IG) The evaluator verifies that end-to-end security is provided without communication protocol security being in place (AG)	Refinement of ADV_FSP.3
The evaluator verifies the correct protection for the different application categories of data in commands, responses and alerts (AG)	Implicit in testing of FDP_IFC.1/Msgs, FDP_IFF.1/Msgs + refinement of ADV_ARC.1, ADV_FSP.3, ADV_TDS.2
The evaluator modifies the context of messages at system level and then checks the validation based on the specified validation rules.	Implicit in testing of FDP_IFC.1/Msgs, FDP_IFF.1/Msgs + refinement of ATE_IND.2
C: Availability of the system (AMI components and communication network) SHALL be sufficient to perform the Use Cases the system has been designed for	
The manufacturer provides design evidence ensuring that the Use Cases are supported. Design evidence is at a level of detail that	Implicitly covered by specific details in the other requirements.

Minimum Security Requirement	SAR/EAL note
enables easy verification… (IG) The evaluator checks the documentation (AG)	
The manufacturers of the components provide standardized failure statistics, MTBF (mean time between failures) or others… (IG) The evaluator checks the failure statistics (AG)	Not mapped (no direct correlation to scope of evaluation or SFRs).
Supervision of the availability of the AMI components and the communication network is implemented The communication network operator provides statistics on the reliability of the message exchange in the network… (IG) The evaluator checks the output of supervision functions and the network statistics (AG)	Not mapped (no direct correlation to scope of evaluation or SFRs, applicable instead to AMI system level).
The manufacturer implements and documents error recovery capabilities for the system and its components… (IG) The availability and recovery is tested by inducing communication and component failures (AG)	Implicit in testing of FPT_BST.1, FPT_FLS.1 + refinement of ADV_FSP.3, AGD_OPE.1
The effect of communication failures is documented… (IG) The evaluator checks the documentation (AG)	Refinement of ADV_FSP.3, AGD_OPE.1
Software protection measures are included in the design process (e.g. by applying the MISRA rules)… (IG) The evaluator checks the software design procedures (AG)	Refinement of ADV_ARC.1, ADV_TDS.2, AGD_OPE.1
D: Crypto mechanism and key management SHALL be documented and be compliant with recognized/proven and approved open standards	
The manufacturer provides design evidence ensuring that this requirement is addressed. Design evidence is at a level of detail that enables easy verification… (IG) The evaluator checks the documentation (AG)	Refinement of ADV_FSP.3
The mechanisms providing encryption and authentication considers NIST recommended (or NSA suite B) cryptography suitable for AMI applications… (IG) The evaluator checks the documentation (AG)	Refinement of ADV_FSP.3, ADV_TDS.2
Documentation SHALL include all implemented features, in particular: - Cryptographic algorithms - Key and signature length - Client/server authentication - Specification of entropy	Refinement of ADV_FSP.3, ADV_TDS.2

Minimum Security Requirement	SAR/EAL note
- Cryptographic Random Number Generation - Storage of keys … (IG) The evaluator checks the documentation (AG)	
E: Every AMI component SHALL check the authorisation of any entity requesting access to it and grant or deny access based on the result of that check	
The manufacturer provides design evidence ensuring that this requirement is addressed. Design evidence is at a level of detail that enables easy verification… (IG) The evaluator checks the documentation (AG)	Implicit in analysis of FDP_IFC.1/Msgs, FDP_IFF.1/Msgs, FDP_IFC.1/Keys, FDP_IFF.1/Keys + refinement of ADV_FSP.3, ADV_TDS.2
This requirement [that every data point and function has defined access rights] is verified in a functional security test. The test specifically ensures that each entity has only the defined and necessary privileges (AG)	Implicit in testing of FDP_IFF.1/Msgs, FDP_IFF.1/Keys + refinement of ATE_IND.2
The manufacturer provides design evidence ensuring that [the sub-requirement that every entity SHALL be uniquely identifiable] is addressed. Design evidence is at a level of detail that enables easy verification… (IG)	Refinement of ADV_FSP.3
The evaluator tests the denial of access mechanism (AG)	Implicit in testing of FIA_AFL.1, FMT_SMF.1, FMT_MOF.1 + refinement of ATE_IND.2
The evaluator changes the clock date/time and tests the denial of access [that applies a specific time after authorisation] (AG)	Implicit in testing of FIA_UAU.6, FMT_MOF.1 + refinement of ATE_IND.2
F: Data at rest SHALL be protected in all system components	
The manufacturer provides design evidence ensuring that this requirement is addressed. Design evidence is at a level of detail that enables easy verification… (IG) The evaluator checks the documentation (AG)	Implicit in analysis of FDP_ACC.2, FDP_ACF.1 + refinement of ADV_TDS.2
The evaluator checks the deletion function (AG)	Implicit in testing of FCS_CKM.4, FDP_RIP.1 + refinement of ATE_IND.2
Make modifications and inspect the log file (AG)	Implicit in testing of FAU_GEN.1 + refinement of ATE_IND.2
G: AMI components SHALL be upgradable to incorporate new (security) functionalities	
The manufacturer provides design evidence ensuring that this requirement is addressed. Design evidence is at a level of detail that enables easy verification… (IG) The evaluator checks the documentation (AG)	Implicit in analysis of FPT_TSU.1 + refinement of ADV_ARC.1, ADV_FSP.3

Minimum Security Requirement	SAR/EAL note
The evaluator performs an update (with valid and invalid images), activates and checks the result [this is a test of the basic capability to fix bugs and upgrade functionality] (AG)	Implicit in testing of FPT_TSU.1 + refinement of ATE_IND.2
The evaluator checks the documentation [for spare memory and processing capacity for upgrades] (AG)	Refinement of AGD_OPE.1
The evaluator performs an update (with valid and invalid images [in terms of authenticity]), activates and checks the result (AG)	Implicit in testing of FPT_TSU.1 + refinement of ATE_IND.2
H: Functionalities in AMI components SHOULD be limited to the intended operational Use Cases and SHALL not be able to compromise security functions	
The manufacturer provides design evidence ensuring that this requirement is addressed. Design evidence is at a level of detail that enables easy verification… (IG) The evaluator checks the documentation (AG)	Implicit in analysis of FDP_IFC.2/Int, FDP_IFF.1/Int + refinement of ADV_FSP.3, ADV_TDS.2
The function to disable interfaces [that are not used] is implemented… (IG) The evaluator disables interfaces and verifies the status of each disabled interface (AG)	Implicit in testing of FDP_IFC.2/Int, FDP_IFF.1/Int + refinement of AVA_VAN.2
The system is designed in such a way that functionality blocks do not interfere with security functions in an unintended way… (IG) The evaluator checks the effect on security by disabling functionalities (AG)	Addressed indirectly by ADV_TDS.2, AVA_VAN.2
I: AMI components and the communications network SHALL be adequately protected against external disturbances and/or attacks and SHALL demonstrate resilience against attacks	
The evaluator checks the documentation (AG)	ADV_ARC.1, ADV_FSP.3, ADV_TDS.2, AGD_OPE.1
The evaluator carries out penetration and other protection testing (AG)	ATE_IND.2, AVA_VAN.2

Table 9 – Minimum Requirements – Assurance Requirements Mapping