Wasion

Security Target

WASION aMeter100 and aMeter300 Smart Energy Meters
Evaluation Assurance Level (EAL): EAL3 augmented with ALC_FLR.3.

TOE Full Name:	Wasion aMeter100 and aMeter300 Smart Energy Meters
Version	v1.6
Date	2025-05-19
Classification:	PUBLIC

Version history

Version	Date	Author	Description
v1.0	2024-05-09	Wasion	The first version of the Security Target.
v1.1	2024-07-25	Wasion	1 Add the information of Pre-established (102) client. 2 The Supervisor client name change to Operator. 3 Revise some descriptive errors. 4 ST version increase to v1.1, 20240715. 5 Amendments based on the 1st analysis cycle
v1.2	2024-09-19	Wasion	1 Change the TOE reference name. 2 Amendments based on the 2nd analysis cycle.
v1.3	2024-12-05	Wasion	Amendments based on AGD 2nd analysis cycle and ST 3rd analysis cycle
v1.4	2025-03-11	Wasion	Amendments based on ASE 3rd analysis cycle, AVA 1st analysis cycle and ATE 2nd analysis cycle.
v1.5	2025-04-08	Wasion	Amendments based on ASE 5th and ADV 3rd analysis cycle
v1.6	2025-05-19	Wasion	New OBIS list version reference

Table of Contents

1 Introduction

1.1 ST References

Table 1 – ST Reference

ST Title	Security Target WASION aMeter100 and aMeter300 Smart Energy Meters
ST Version	v1.6
ST Creation Date	2025-05-19

1.2 TOE Reference

Table 2 – TOE Reference

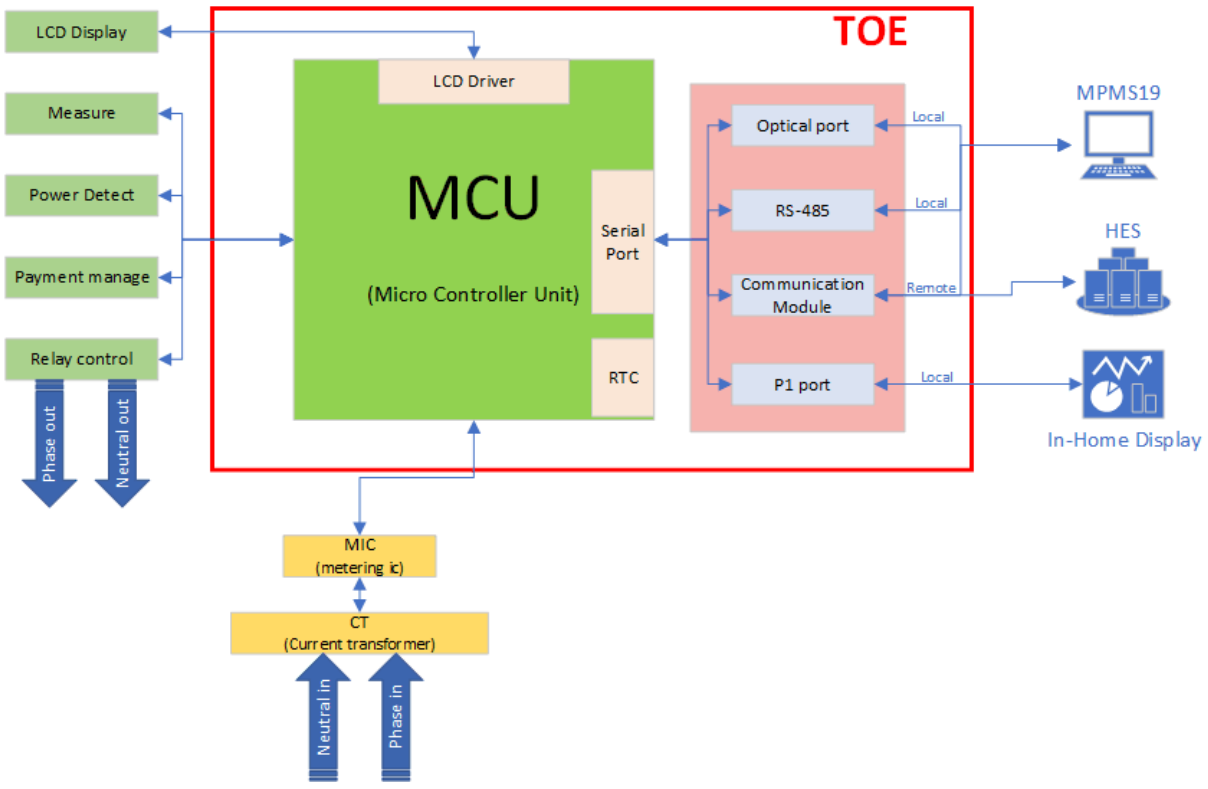
TOE Full Name	Wasion aMeter100 and aMeter300 Smart Energy Meters
TOE Version	See Table 3 - TOE versions
TOE Short Name	Wasion Smart Meter

1.3 TOE Overview

The meter takes digital medium as information exchange media. The meter can realize remote communication and control via CAT-1/CAT M1 module. Meantime, it also supports DLMS/COSEM specification to achieve interconnection with the master station. The meter includes measurement unit, display unit, button input unit, real-time clock unit, infrared communication, remote communication, load switch and other auxiliary equipment.

1.3.1 TOE Boundary

Figure 1 – TOE Boundary



Wasion Smart Meter includes two types of devices based on the metrology. Different power supply needs different metrological systems. The aMeter100 is a single-phase, while the aMeter300 is a three-phase smart meter. The evaluation related FW parts are identical in both configurations [EQ-Report].

The firmware has 3 parts:

1. Metrology (legal)
2. Functionality and security (application, non-legal)
3. BootLoad

Table 3 - TOE versions

Type	aMeter100	aMeter300
Hardware version	DDZ101-aMeter100(GTEU)V1.0	DTZ341-aMeter300(GTEU)V1.0
Firmware version of part 1	aM100-L-A3480100	aM300-L-B3480100
Firmware version of part 2	aM100-N-A3480100	aM300-N-B3480100
Firmware version of part 3	Wasion-aMeter-BOOT-V1.0-20231125	Wasion-aMeter-BOOT-V1.0-20231125

An AMI usually contains at least an intelligent measurement device, in our case smart meter, and a Head-End System (HES).

The TOE has following interfaces:

- Optical port, which can support direct HDLC or Mode E(IEC 62056-21).
- RS485 port, which can support direct HDLC.
- Communication Module (CAT-1/CAT M1), which can support IEC 62056-47.
- P1 port, which can support Mode D (IEC 62056-21), physical connector pin assignment of passive mode according to DSMR5.0.2.

1.3.1.1 Checksum calculation and algorithm

The firmware of the meter is stored in the Flash memory inside the MCU. During the manufacturing process, the firmware is pre-installed in the Flash through burning, and the hardware does not have an interface for firmware debugging/burning. Therefore, if the program needs to be updated later, it can only be done through remote upgrading; direct burning is not feasible.

When performing a remote upgrade, only upgrade images with ECDSA P-256 digital signatures are accepted, and CRC32 type upgrade images are rejected.

Since the MID certification prototype requires displaying the firmware's checksum, which is generally in the form of a CRC32 value, the legally required procedures and non-legally required procedures both used CRC32 values to fill in the signature area during the original MID certification process. Because no changes are allowed to the measurement parts of the firmware after MID certification, the signature area of the CC certification prototype is the same as that of the MID certification prototype, which uses CRC32 values.

In summary, the points are as follows:

1. Although the firmware of the certification prototype has CRC32 values filled in the signature area, this is only to meet the MID certification requirements for display and reading purposes and does not mean that upgrade images signed with CRC32 can be used for upgrading.

2. Currently, there is only one way to upgrade the firmware, which is to use upgrade images with ECDSA P-256 digital signatures for remote upgrading. Other methods are not feasible

1.3.2 TOE Type

Wasion Smart Meter is designed with high quality refer to international standard for advanced metering infrastructure. A smart meter is an electronic device that records information such as consumption of electric energy, voltage levels, current, and power factor. Smart meters communicate the information to the consumer for greater clarity of consumption behaviour, and electricity suppliers for system monitoring and customer billing.

1.3.3 TOE Usage and Major Security Features

The main usage function of the TOE:

- Energy measurement, including active, reactive energy and each tariff energy.
- Support DLMS/COSEM and IDIS2.0 specification to realize interconnection with master station.
- Event detection and record. (Event Recording Function)
- Remote communication. The master station can read meter data by CAT-1/CAT M1 communication.
- Data display, including meter LCD display.

1.3.3.1 Security of local measurement data

The TOE has tamper protection. The memory of the TOE is located under the cover. The memory can therefore only be accessed by physical disassembly. The protection system can be divided into two parts. The first part is a sealable that can be placed on the screws, which prevents the screw from rotating. If someone removes this sealed, there will be a physical trace of intrusion. The second part of protection is that the TOE covers are assembled and connected to a physical switch. This switch can send a signal to the TOE that the cover has been removed. The signal is stored by the TOE with a reliable time stamp, so that the removal the cover can be accurately traced back.

1.3.3.2 Secure communication

The TOE supports DLMS/COSEM high level security communication. This means it uses the following encryption:

- (0) AES-GCM-128 for authenticated encryption and AES-128 for key wrapping.
- (1) AES-GCM-128 authenticated encryption, ECDSA P-256 digital signature, ECDH P-256 key agreement, SHA-256 hash and AES-128 key wrapping.

1.3.4 Non-TOE Software/Firmware/Hardware

List of the software/hardware/firmware that are not part of the TOE but are required for the operation and secure usage of the TOE.

- Parameter Management System Version: V1.0.9.hu – A usual AMI (Advanced Metering Infrastructure) contains a Head-End System (HES) to manage the devices in the system. Since Parameter Management System has all the functionality as a HES related to the evaluation, there is no HES in the TOE environment.
- Optical cable that supports the IEC 62056-21 standard.
- Local access to the TOE, because of the optical cable and P1 connection.

1.4 TOE Description

This section primarily addresses the physical and logical components of the TOE that are included in the evaluation.

1.4.1 Physical Scope of the TOE

The outer cover of the TOE consists of polycarbonate. The positive property of polycarbonate is that it can withstand UV and temperature as well. The outer cover is completely modular, so it consists of several parts. These parts can be fixed with lockable screws. The following picture shows the outer cover of the TOE and an explanation the next table.

Figure 2 - TOE structure (aMeter100)

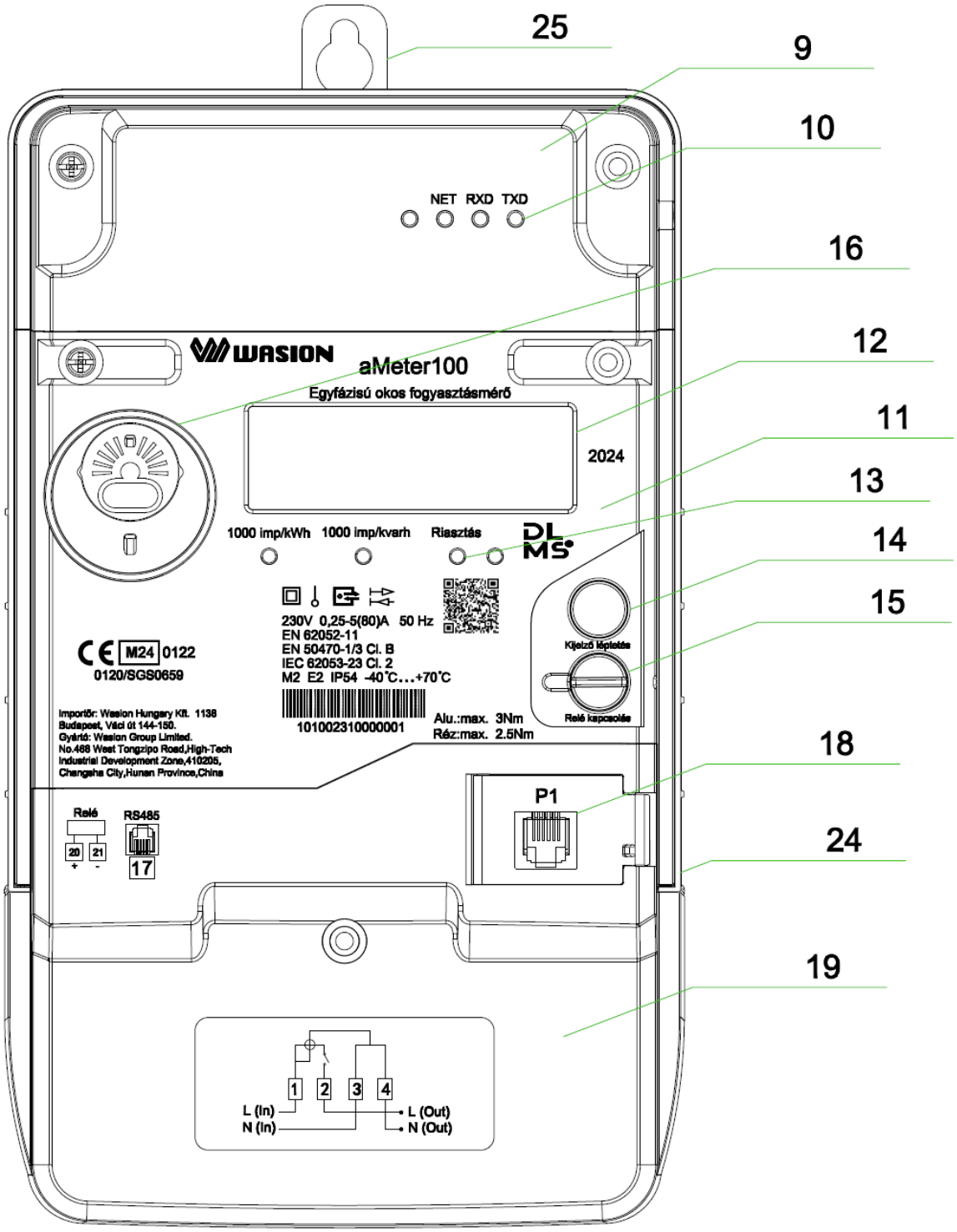


Figure 3 - TOE structure (aMeter300)

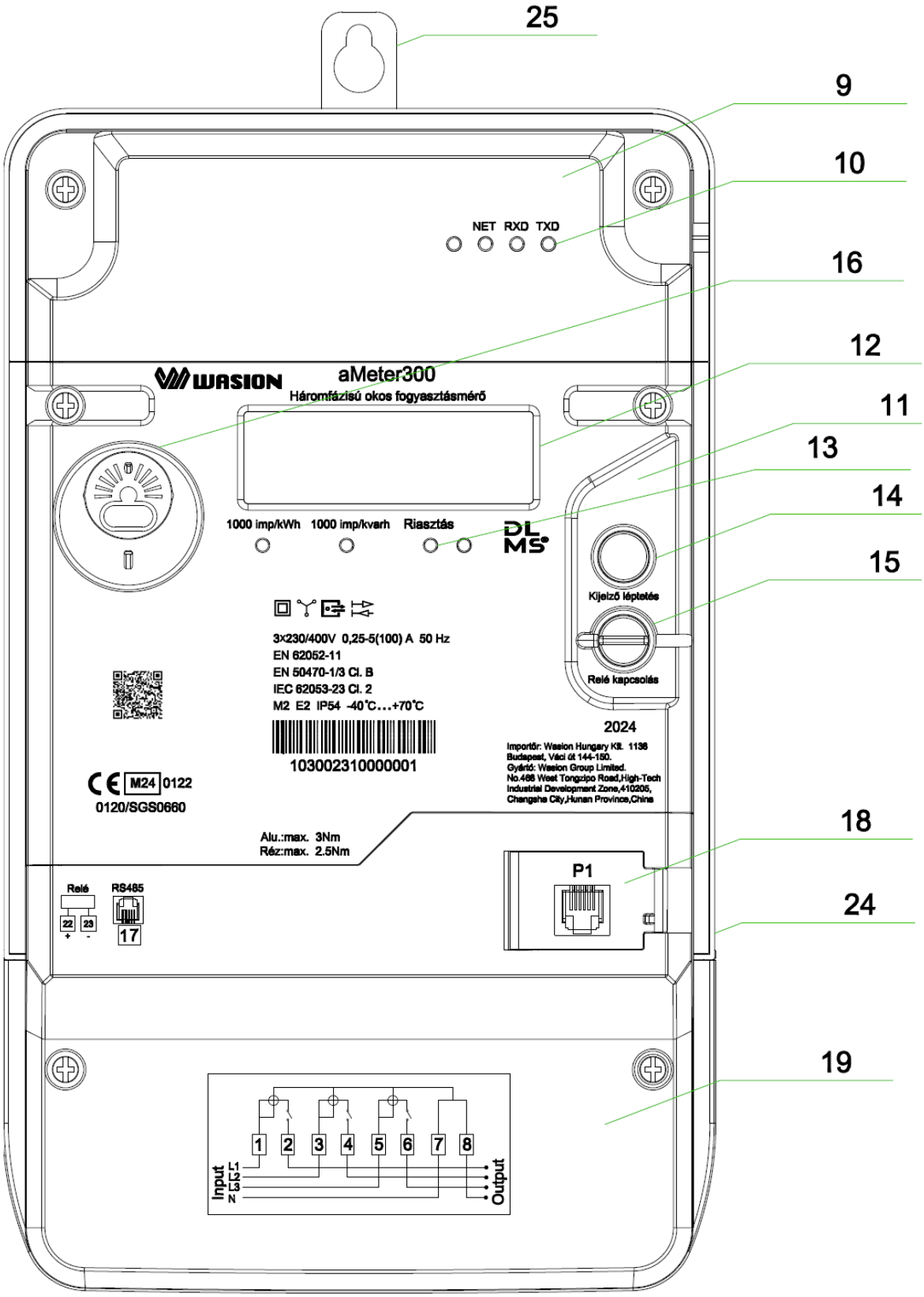


Table 4 - TOE components

Number	Component	Number	Component
1/2/3/4	Terminal Block LLNN (under the Terminal Cover)	1/2/3/4/5/6/7/8	Terminal Block L1L1L2L2L3L3NN (under the Terminal Cover)
9	Module Cover (Include Battery Replace)	10	Module status (NET/RXD/TXD)
11	Meter Cover	12	LCD Area
13	Active Pulse LED/ Reactive Pulse LED/ Alarm LED	14	Display Scroll Button
15	Relay Control Button	16	Optical Port
17	RS485 (RJ45) (under the Terminal Cover)	18	P1 Port
19	Terminal Cover	20/21/22/23	Auxiliary Relay (under the Terminal Cover)
24	Meter Base	25	Hang

The unnumbered and/or unidentified texts on the picture are labels on the TOE housing based on the customer's requirements. The figure below is a realistic picture of the TOEs, the slight differences in the texts does not affect the unique identification, the critical information is always there (e.g., serial number, manufacturer, type, etc.).

Figure 4 - TOE photorealistic picture

The meter supports local update via local communication port (IR or RS485) or remote ports (GPRS or G3-PLC) and adopts DLMS to upgrade meter’s firmware. The meter will auto execute

the new program after updating. During the process of remote update, the meter must keep power-on. The firmware upgrade shall be as according to DLMS.

1.4.1.1 Delivery of the TOE

The manufacturer strict and well-controlled manufacturing processes guarantee that only a proper product (that went through the whole Quality Assurance steps) can reach the delivery phase, like automatic manufacturing steps, testing at several stages. The delivery of the products to the customer is done in mass delivery. The procedures assure that the customer will be aware that the evaluated version is shipped to them. The exact delivery is “embedded” into the ordering, secured transport via borders and tracking measures.

When the customer receives the product, physical and procedural checks can be done.

1.4.1.2 Guidance documents

- User Manual pdf for aMeter100 and aMeter300, [UM]
- AGD Documentation Wasion Smart Meter (aMeter100 and aMeter300), [AGD]

The type of all documents is PDF format.

1.4.2 Logical Scope of the TOE

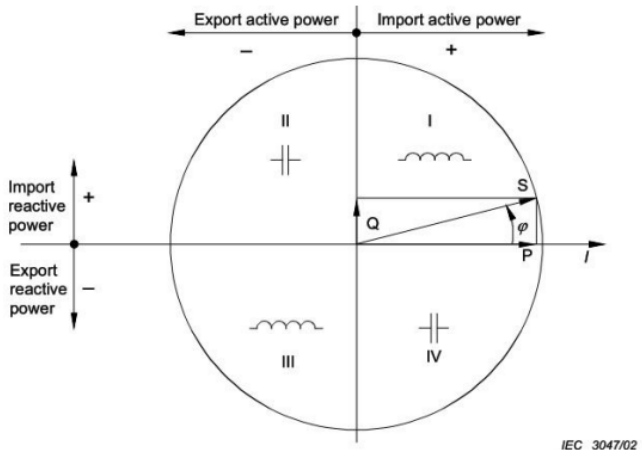
The TOE provides a combination of the following meter-related functions:

- Metrology functions that are under legal metrological control are SFR non-interfering functions
  - Energy
  - Demand
  - Display
  - Battery
  - TOU
  - Profile
  - Relay-Control
- Functions and features in the logical scope of the TOE
  - Real-Time Clock
  - Event log
  - Push
  - Firmware upgrade
  - Security
  - Meter communication, including network interfaces and direct interfaces
    - Optical Port
    - RS485
    - Communication Module
      - CAT1/CAT M1
    - P1 Port

1.4.2.1 Energy

Its measurement capability consists of passing the incoming phase through a measurement point and, after the measurement has been made, it transmits the current through the output phase. The energy measurement can be seen in the following picture:

Figure 5 - Geometric representation of active and reactive power



Geometric representation of active and reactive power

The active and reactive energy is calculated according to the formulas as below:

$$\text{Active Energy} = \int_0^t V(t)I(t)\cos\varphi(t)dt$$

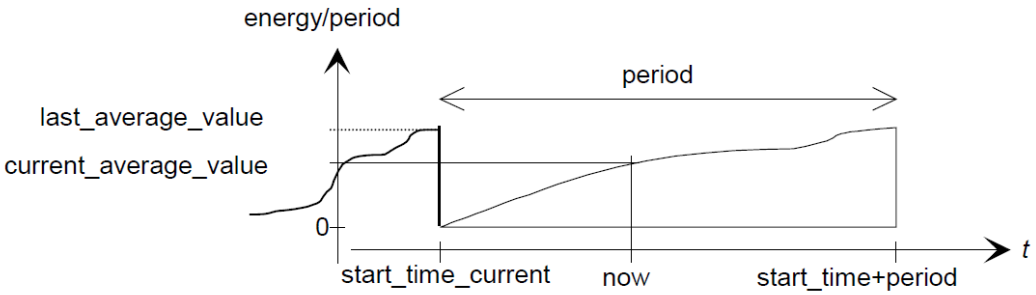
$$\text{Reactive Energy} = \int_0^t V(t)I(t)\sin\varphi(t)dt$$

This method is precise at low current.

1.4.2.2 Demand

The demand period can be set between 1 and 15. The demand time can be set to 60/300/900/1800/3600 seconds.

Figure 6 - Demand



1.4.2.3 TOU

The following instances allow the management of the tariff.

Table 5 - TOU

Item	Class	OBIS
Clock	Class Id 8	Logical name 0-0:1.0.0.255
Activity calendar	Class Id 20	Logical name 0-0:13.0.0 255
Special days table	Class Id 11	Logical name 0-0:11.0.0.255
Energy Register activation	Class Id 6	Logical name 0-0:14.0.1.255
Maximum Demand Register activation	Class Id 6	Logical name 0-0:14.0.2.255
Tariffication script table	Class Id 9	Logical name 0-0:10.0.100.255
Current active tariff	Class Id 1	Logical name 0-0:96.14. 0.255

1.4.2.4 Real-Time Clock

The meter equipped a RTC module, the module will manage the whole time.

1.4.2.5 Display

Meter equipped a HTN positive LCD to display information, operating and storage temperature from -40℃ to 70℃,and image clarity for 20 years. There are two optional LCD according to customer's requirement.

1.4.2.6 Profile

Meter equipped non-volatile memory EEPROM and data flash to store electric data for 20 years when meter is no power.

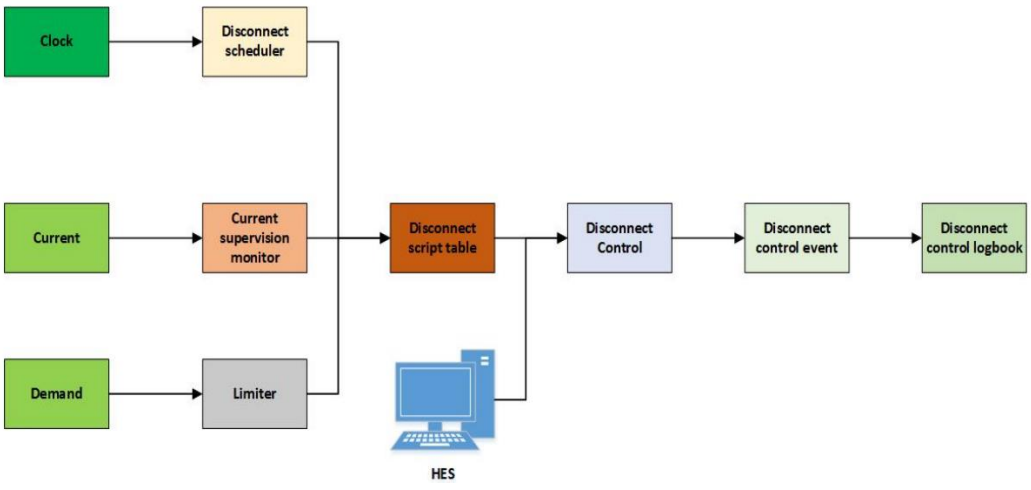
There are 4 periods:

- End of Billing Period 1
- End of Billing Period 2
- Load Profile with Period 1
- Load Profile with Period 2

1.4.2.7 Relay control

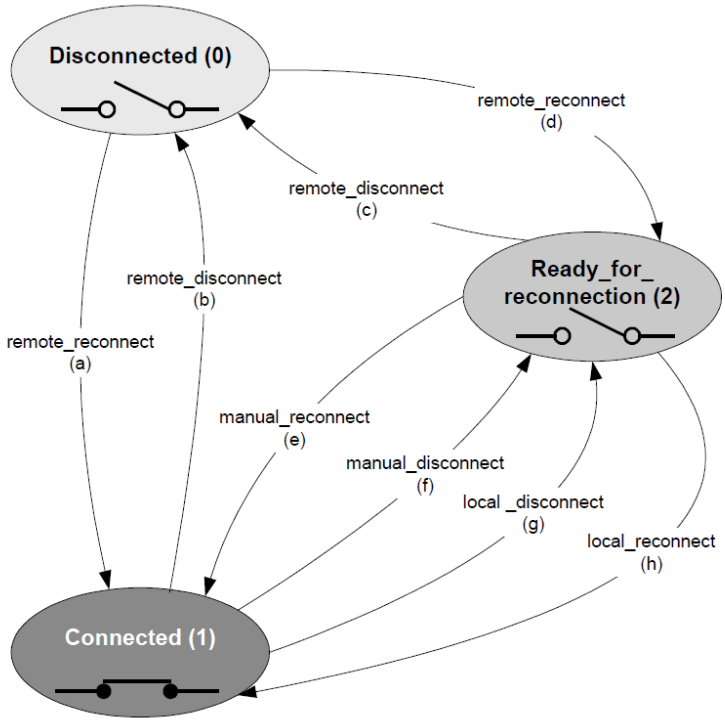
The full section related to the Connection / Disconnection management applies with the restrictions below. Scheduled disconnection / reconnection is managed using the Disconnect control scheduler instance. Only a full specified execution time is allowed in the attribute 4 of object "Disconnect Control Scheduler" instances of class 22. No wild card leading to periodic disconnection is permitted.

Figure 7 - Relay control flaw chart



The disconnect control object is as defined in the DLMS 1000-1 [B-Book]. The disconnect control state diagram is as followed:

Figure 8 - Disconnect control



1.4.2.8 Event Log

The meter supports several logbooks including

Table 6 - Event logs

Logbooks	OBIS	Minimum capacity
Standard Event Log	0-0:99.98.0.255	500
Fraud Detection Log	0-0:99.98.1.255	200
Communication log	0-0:99.98.5.255	200
Disconnector Control log	0-0:99.98.2.255	200
Power Quality Log	0-0:99.98.4.255	200
Power Failure Management	1-0:99.97.0.255	200

1.4.2.9 Security

The TOE can distinguish users. Different users can be associated with different roles. The following image summarizes the roles and their associated rights.

Table 7 - Profiles

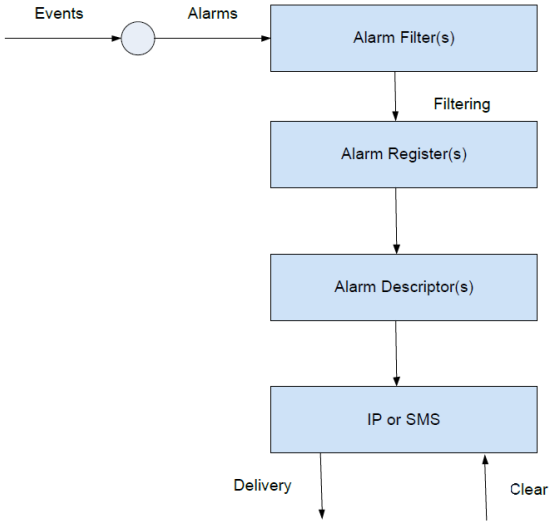
Client	Client SAP	Behavior	Services supported by a Server
Administrator	1	Read all data Configure all parameters Method all	· Block-transfer-with-get · Block-transfer-with-set · Get · Set · Multiple-references · Selective Access · Action · General-block-transfer · General-protection

Operator	111	Read all data Configure all parameters Method all	· Block-transfer-with-get · Block-transfer-with-set · Get · Set · Multiple-references · Selective Access · Action · General-block-transfer · General-protection
Reader	112	Read all data	· Block-transfer-with-get · Block-transfer-with-set · Get · Set · Multiple-references · Selective Access · Action · General-block-transfer · General-protection
Pre-established	102	Configure partial parameters Method partial Push	· Set · Action · Data-Notification · General-block-transfer · General-protection
Public	16	Read partial data(COSEM logic name, Billing period counter, Security Receive frame counter, Association, SAP Assignment)	· Block-transfer-with-get · Get

1.4.2.10 Push

Some of the events can trigger alarms. If one of these events occurs, the corresponding flag in the alarm registers is set and an alarm is then raised via communication channel. All alarm flags in the alarm registers remain active until the alarm registers are cleared. Each bit in the alarm registers represents a different alarm. If the bit is set (logical 1) the alarm (corresponding to position of the set bit) was recorded. The value in the Alarm Registers is a summary of all active and inactive alarms at that time. Depending on the capabilities of the system and the policy of the utility, not all possible alarms are wanted. Therefore, the Alarm Filters can be programmed to mask out unwanted alarms. The structure of the filter is the same as the structure of the Alarm Registers. To mask out unwanted alarms the corresponding bits in Alarm Filters should be se to logical 0.

Figure 9 - Alarm push



1.4.2.11 Firmware upgrade

The TOE can upgrade the firmware. This ability can be activated both remotely and locally. First, the firmware image must be sent to the TOE. After the firmware image has been successfully received, it is then identified and verify the signature by the TOE. After the TOE has found everything in order and created the logs and it performs a firmware upgrade.

The following instances allow the management of the firmware upgrade:

Table 8 - Firmware upgrade classes

Name	Class ID	OBIS code
Image transfer	Class Id 18	Logical name 0-0:44:0.0.255
Active firmware identifier	Class Id 1	Logical name 1-0:0.2.0.255
Active firmware signature	Class Id 1	Logical name 1-0:0.2.8.255
Clock	Class Id 8	Logical name 0-0:1.0.0.255
Image activation script table	Class Id 9	Logical name 0-0:10.0.107.255
Image activation single action scheduler	Class Id 22	Logical name 0-0:15.0.2.25
Standard logbook event	Class Id 1	Logical name 0-0:96.11.0.255
Standard logbook	Class Id 7	Logical name 0-0:99.98.0.25

1.4.2.12 Communication Interface

Meter has optical port, which can support direct HDLC or Mode E (IEC 62056-21).

Optical, RS-485, Cellular communication interface:

- Type: Serial bi-direction communication interface
- Baud rate: 9600bps
- Application: Data reading and related data item configuration
- Pattern: Non-modulated IR communication or RS485 or CAT-1/CAT M1

P1 communication interface:

- Type: Serial unidirectional communication interface
- Baud rate: 115200bps
- Application: Data readout

- Pattern: P1

1.4.2.13 Battery

The meter is equipped with a replaceable and an internal non rechargeable 1200 mAh batteries according to requirement. The replaceable battery is protected by the module cover. So, it can be changed without open the meter cover. When the power grid is cut off, the system turns on standby batteries to maintain the clock of the meter and record events.

2 Conformance Claims

Table 9 - Conformance Claims

Common Criteria Conformance	Common Criteria for Information Technology Security Evaluation, CC Part 2 extended, CC Part 3 conformant
Common Criteria version	Version 3.1 Revision 5
PP Conformance	[SM_MSR] PP strict conformance
Evaluation Assurance Level	EAL3 augmented with ALC_FLR.3

This Security Target claims to be Common Criteria Part 2 extended and Common Criteria Part 3 conformant and written according to the Common Criteria version 3.1 R5 [CC_P1], [CC_P2] and [CC_P3].

This Security Target conforms to Protection Profile for Smart Meter Minimum Security requirements. The PP require strict conformance.

This ST conforms to assurance package EAL3 augmented by ALC_FLR.3 defined in [CC_P3].

3 Security Problem Definition

This section defines the security problem to be addressed by the TOE and its operational environment and includes the following:

- External Entities and Threat Agents.
- Assets
- Secure Usage Assumptions,
- Threats, and
- Organisational Security Policies (OSPs).

3.1 External Entities and Threat Agents

Direct Users: Users who interact physically with the meter via a separate component connected to the meter by a direct interface.

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

The SFRs in this Security Target has define specific roles or privileged operations on the meter[1]. Such role might be that of a service technician who carries out any installation, commissioning, maintenance, or diagnostic activities on the meter: for the purposes of this Security Target such users are treated as direct or network users depending on the interfaces that they use to interact with the TOE. It is also possible that service technicians may need access to privileged functions, so all such functions are included in this 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. Any user role defined in section 6.3.5.1 Security roles can be used via a direct or network connection.

3.2 Assets

Table 10 - Assets

Asset	Description	Need for protection
Meter data	consumption, credit, load profile, event log, billing data. etc…	According to their specific need
Configuration data	keys and configurations of other function.	Integrity. Authenticity
Operating parameters	measurement calibration data	Integrity. Authenticity
Meter controls	disconnection the internal relay to disable supply of the energy.	Authenticity
Correct operation of the meter	meter operation without any irrecoverable fault	According to their specific need
Meter Clock	date and time of the real time clock of Meter, Meter clock is used to TOU function, load profile and event logs records.	Integrity. Authenticity(Adjusted clock).
Personally identifiable information	Personally identifiable Information refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.	Confidentiality
Firmware update	Firmware update that is transferred by the Parameter Management System Version: V1.0.9.hu to update the firmware of the TOE.	Integrity and authenticity

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

[1] 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.

the TOE, or obtaining a key that enables access to such data. The types of data are not separately defined in here 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[2].

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 Security Target.

3.3 Assumptions

Table 11 - Assumptions

Assumption	Description
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.
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 (Application Note 3 from [SM-MSR])* The audit trail consists of the log of security events recorded by the TOE.
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 (Application Note 4 from [SM-MSR])* 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.

[2] The types of data are defined in this Security Target by the completion of rules in FDP_ACF.1 and FDP_IFF.1/Msgs.

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 [SM-MSR].)

3.4 Threats

3.4.1 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.

3.4.2 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).

3.4.3 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 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.

3.4.4 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).

3.4.5 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.

3.5 Organizational Security Policies

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

Table 12 - OSPs

OSP	Description
OSP.Logging	**Logging security events** The TOE shall maintain a log of security events and shall protect the log against unauthorised modification. *Application Note 1 (Application Note 1 from [SM-MSR])* This log is required to assist in diagnosis of faults, determination or confirmation of the meter state, and investigation of suspicious events.
OSP.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 (Application Note 2 from [SM-MSR])* The specific destinations and events are not specified in the Protection Profile but are defined by the ST author[3].

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.

Table 13 - Security Objectives for the TOE

Objective	Description
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

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

	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.
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.
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.
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 (Application Note 5 from [SM-MSR])* 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).
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.
O.Resilience	**Resilience against failures** The TOE shall start-up and recover from failures in a defined and secure way.
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 (Application Note 6 from [SM-MSR])*

	The term “firmware” is used in this security target 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.
O.Logging	**Security event logging** The TOE shall maintain a log of security events and shall protect the log against unauthorised modification.
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.

Table 14 - Security Objectives for the Operational Environment

Objective	Description
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.
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.
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.
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 [SM-MSR].)

4.1 Security Objectives Rationale

This section demonstrates that the stated security objectives counter all identified threats, enforce policies, and uphold assumptions.

The following table provide a mapping of security objectives for the TOE and security objectives for the operational environment of the TOE to the defined threats, policies, and assumptions, illustrating that each security objective covers at least one threat, enforces a policy or upholds an assumption and that each threat, policy or assumption is covered by at least one security objective.

The tables below provide information regarding:

- the identified security objectives providing effective countermeasures for the threats;
- the identified security objectives providing complete coverage of each organizational security policy;
- the identified security objectives upholding each assumption.

4.1.1 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.

Table 15 – Security objectives coverage

	O.Authorisation	O.Messages	O.DataAtRest	O.Crypto	O.Interfaces	O.Resilience	O.SecureUpdate	O.Logging	O.Alarms		OE.ExternalData	OE.AuditSupport	OE.InspectionSuppor	OE.UniqueSubjectID
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							
OSP.Logging								X						
OSP.Alarms									X					
A.ExternalData											X			
A.AuditSupport												X		
A.InspectionSupport													X	
A.UniqueSubjectIDs														X

4.1.2 Security Objectives Rationale relating to 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[4].
- 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.

4.1.3 Security Objectives Rationale relating to Assumptions

Each of the Assumptions in section 3.3 is directly matched by a security objective for the operational environment in section 4 that list in Table 14 - Security Objectives for the Operational Environment. The wording of each objective for the operational environment includes the wording of each assumption, and no further rationale is therefore given here.

4.1.4 Security Objectives Rationale relating to OSPs

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE.

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.

5 Extended Components Definition

5.1 Conventions

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Refinements are identified using bold text. (Example: **TSF Data**) Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.

5.2 Security Event Alarm (FAU_ARP.2)

This component extends the existing family FAU_ARP in [CC_P2], 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

[4] 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.

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*].

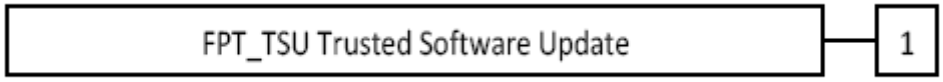
FAU_ARP.2.4 The TSF shall send alarms according to the following timing rules: [assignment: *rules that specify when an alarm must be sent relative to the detection of the event*].

5.3 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:



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 (Application Note 7 from [SM-MSR])

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.

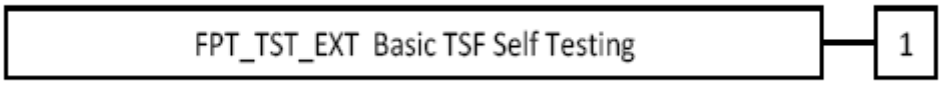
5.4 Basic TSF Self Testing (FPT_BST.1)

The extended component defined here is a simplified version of FPT_TST.1 in [CC_P2].

Family behaviour

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

Component levelling:



Management: FPT_BST.1

There are no management activities defined by default.

Audit: FPT_BST.1

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

- Indication that TSF self-test was completed.

FPT_BST.1	*Basic TSF Self Testing*

Hierarchical to: No other components.

Dependencies: No dependencies

FPT_BST.1.1 The TSF shall run a suite of the following self-tests [selection: during initial start-up (on power on), periodically during normal operation, 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*].

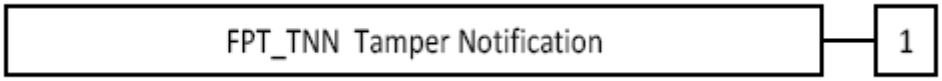
5.5 Tamper Notification (FPT_TNN.1)

The extended component defined here has some similarities with FPT_PHP.2 in [CC_P2] 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 (Application Note 8 from [SM-MSR])

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,

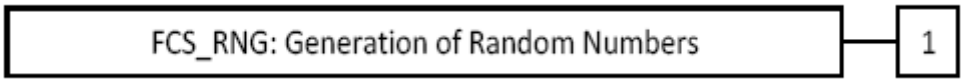
the sending of a particular alarm message, or the recording of a particular log entry. In the case of a log entry, the content of the log entry should be described using an appropriate FAU SFR, and the protection of the log against modification (cf. FAU_STG.1) associated with the tamper event should be described in the TOE Summary Specification.

5.6 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:



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 (Application Note 9 from [SM-MSR])

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 (keystrokes, 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

This section defines the SFRs and SARs met by the TOE.

6.1 Conventions

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Refinements are identified using bold text. (Example: **TSF Data**) Any text removed is stricken and bold (example: ~~**TSF Data**~~) and should be considered as a refinement.
- Iterations are identified by appending a unique identifier starting with a slash following the component title. For example, FDP_IFF.1/Msgs - Simple security attributes, and FDP_IFF.1/Keys Simple security attributes would be the second iteration.
- Assignment and selection operations already performed by the PP are identified using *italicized text without brackets*.
- Refinement operations already performed by the PP are identified using ***italicized bold text without brackets***.

6.2 SFR Architecture

Figure 10 - Architecture of Message Security, TSF Protection and Audit SFRs and Figure 12 - Architecture of Data Protection and Underlying Cryptography SFRs 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 [CC_P2].

Figure 10 - Architecture of Message Security, TSF Protection and Audit SFRs

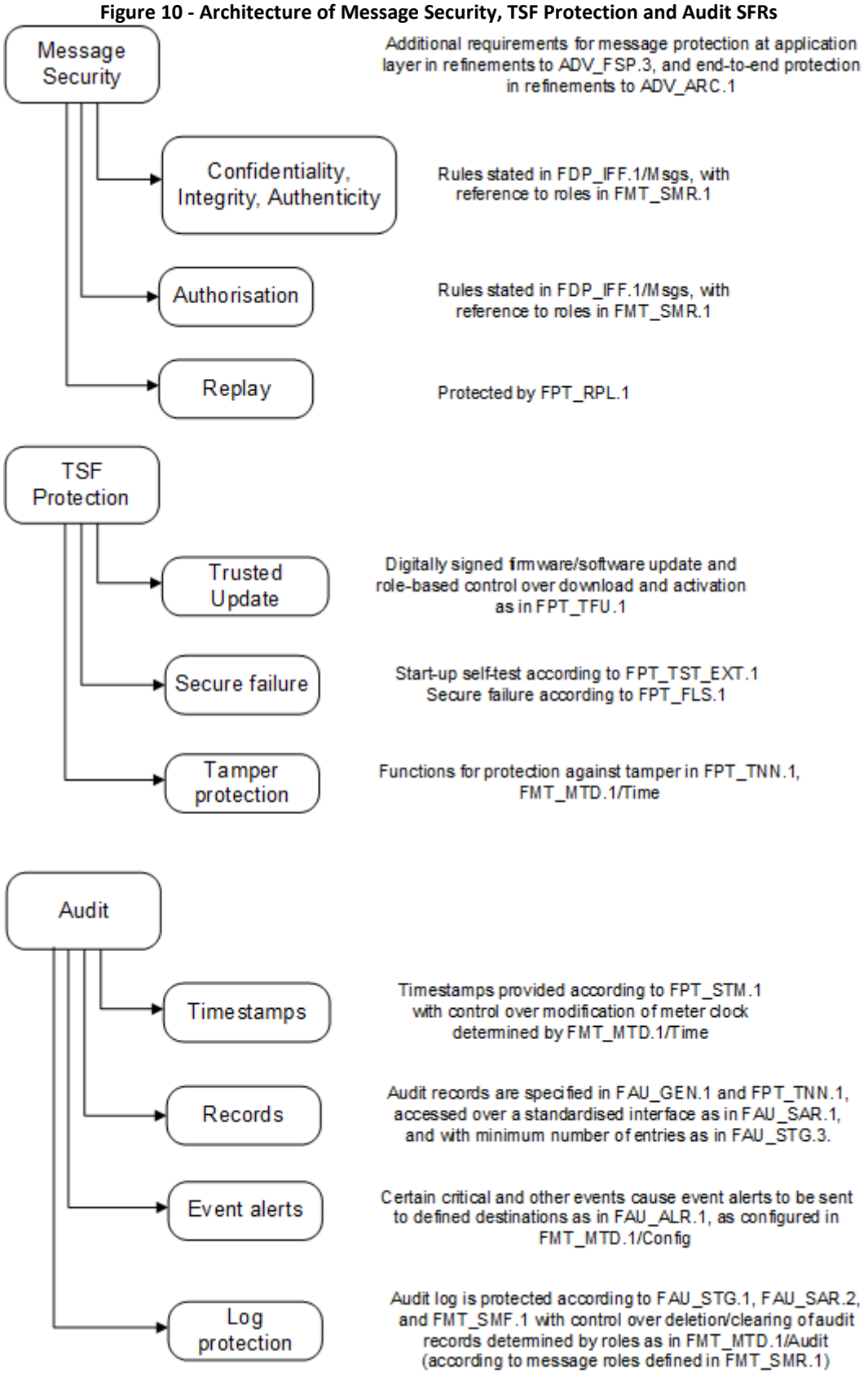


Figure 11 - Architecture of Authentication & Authorisation SFRs

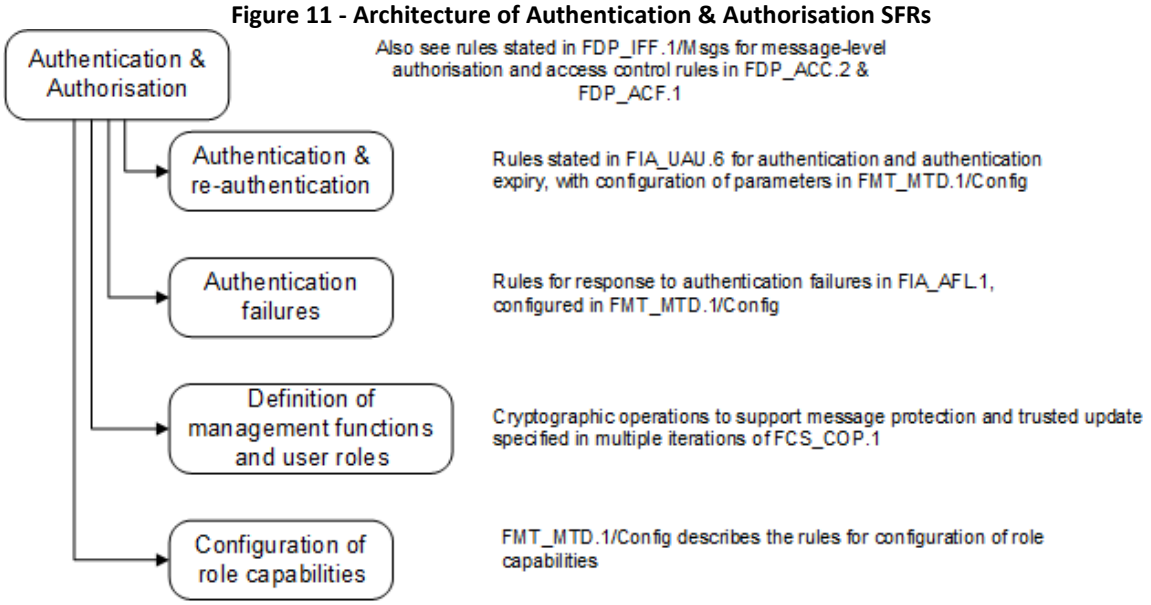
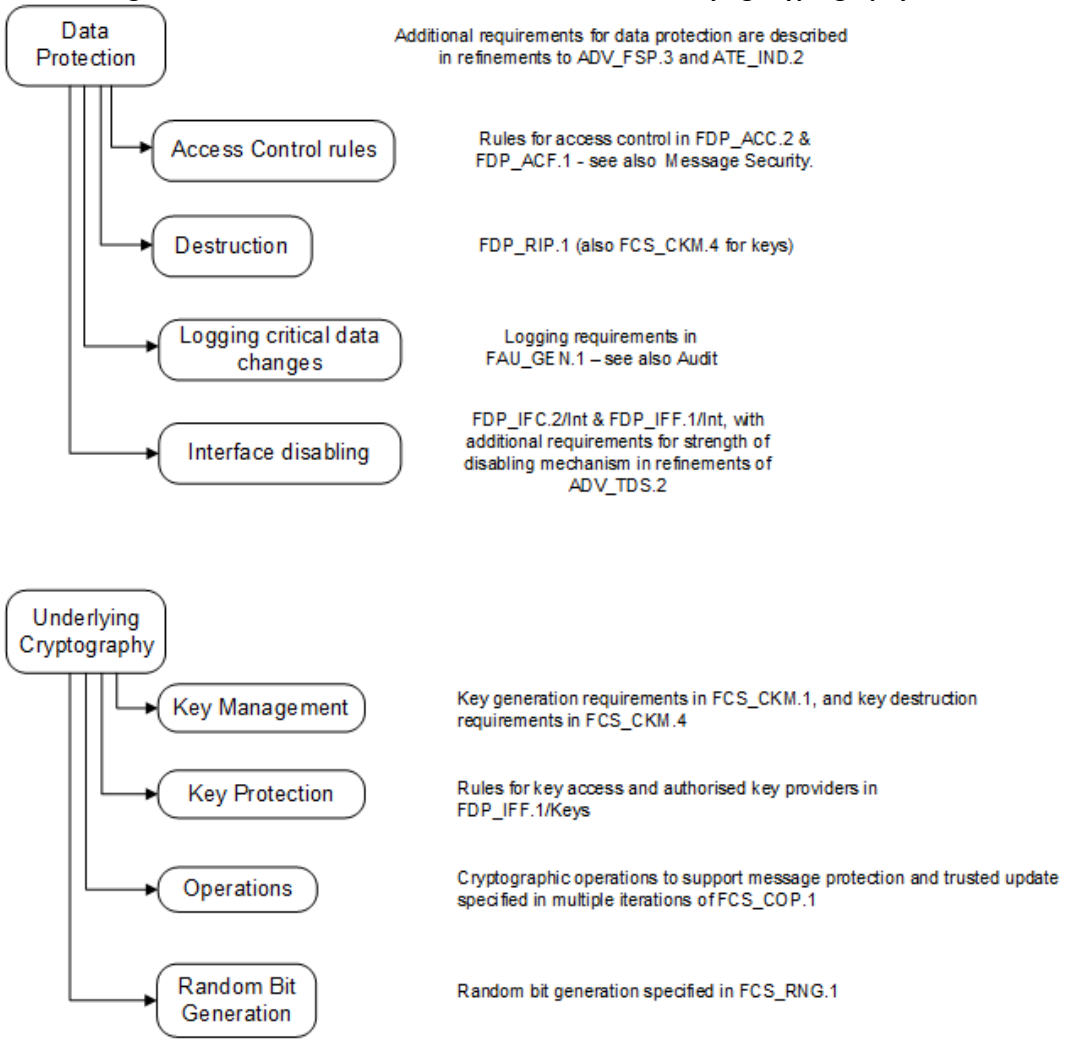


Figure 12 - Architecture of Data Protection and Underlying Cryptography SFRs



6.3 TOE Security Functional Requirements

Table 16 - SFRs

Name	Description	S	A	R	I
FCS_CKM.1	Cryptographic key generation		x		
FCS_CKM.4	Cryptographic key destruction		x		
FCS_COP.1	Cryptographic operation		x		
FCS_RNG.1	Generation of random numbers	x	x		
FDP_ACC.2	Complete access control		x		
FDP_ACF.1	Security attribute-based access control		x		
FDP_IFC.1/Msgs	Subset information flow control – Messages		x		x
FDP_IFF.1/Msgs	Simple security attributes – Messages		x	x	x
FDP_IFC.2/Int	Complete information flow control – Interfaces		x		x
FDP_IFF.1/Int	Simple security attributes – Interfaces		x	x	x
FDP_IFC.1/Keys	Subset information flow control – Keys		x		x
FDP_IFF.1/Keys	Simple security attributes – Keys		x	x	x
FDP_RIP.1	Subset residual information protection	x	x		
FIA_UAU.6	Re-authenticating		x	x	
FIA_AFL.1	Failure with preservation of secure state	x	x	x	
FPT_BST.1	Basic TSF Self Testing	x	x		
FPT_FLS.1	Failure with preservation of secure state		x		
FPT_TNN.1	Tamper notification		x		
FPT_RPL.1	Replay detection	x	x	x	
FPT_STM.1	Reliable time stamps				
FPT_TSU.1	Trusted update	x	x	x	
FMT_SMR.1	Security roles		x	x	
FMT_MOF.1	Management of Security Functions Behaviour	x	x		
FMT_MTD.1/Audit	Management of TSF data – Audit	x	x		x
FMT_MTD.1/Time	Management of TSF data – Time	x	x		x
FAU_ARP.2	Security Event Alarm		x		
FAU_GEN.1	Audit data generation	x	x	x	
FAU_SAR.1	Audit review		x	x	
FAU_SAR.2	Restricted audit review		x	x	
FAU_STG.1	Protected audit trail storage	x		x	
FAU_STG.3	Action in case of possible audit data loss		x		

Note: S = Selection, A = Assignment, R = Refinement, I = Iteration

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 [*AES-128 key wrap,*

ECDH with P-256][5] and specified cryptographic key sizes [*128 bit*][6] that meet the following: [[*RFC 3394*], *[NIST SP 800-56A]*, *[IEC62056-53]*][7].

Application Note 10 (Application Note 10 from [SM-MSR])

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 19).

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 [*zeroization for dedicated key, ephemeral key, client digital signature public key certificate (when no longer needed), client key-agreement public key certificate(when no longer needed)*][8] that meets the following: [[*FIPS 140-2*], *[NIST SP 800-56A], security setup (class_id=64) remove_certificate of [IEC62056-62]*][9].

Application Note 11 (Application Note 11 from [SM-MSR])

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.

[5] [assignment: *cryptographic key generation algorithm*]
[6] [assignment: *cryptographic key sizes*]
[7] [assignment: *list of standards*]
[8] [assignment: *cryptographic key destruction method*]
[9] [assignment: *list of standards*]

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 [*shown in the table below*][10] in accordance with a specified cryptographic algorithm [*shown in the table below*][11] and cryptographic key sizes [*shown in the table below*][12] that meet the following: [*shown in the table below*][13].

Table 17 - Cryptographic operations

Operation	Algorithm	Key size	Standard
Encryption DLMS message encryption	AES-GCM-128	128 bits	[NIST SP 800-38D]
Decryption DLMS message decryption	AES-GCM-128	128 bits	[NIST SP 800-38D]
Secure Hash DLMS generate message digest and Firmware Update generate image digest	SHA-256	-	[FIPS PUB 180-4]
Digital Signature DLMS message signature and firmware update verification	ECDSA with P-256	Public Key:512bits Private Key:256 bits	[FIPS PUB 186-5]
Key wrap	AES-128 key wrap	128 bits	[RFC 3394]
Key Agreement	ECDH with P-256	128 bits	[NIST SP 800-56A]

Application Note 12 (Application Note 12 from [SM-MSR])

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.

[10] [assignment: *list of cryptographic operations*]
[11] [assignment: *cryptographic algorithm*]
[12] [assignment: *cryptographic key sizes*]
[13] [assignment: *list of standards*]

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 [physical][14] random number generator that implements: [*challenges, private key (used with a public key algorithm)*][15].

FCS_RNG.1.2 The TSF shall provide [*numbers [128bit*n]*][16] that meet [[*FIPS 140-2]*][17].

Application Note 13 (Application Note 13 from [SM-MSR])

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.

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*[18] on

(1) subjects: all

(2)objects: metrologically certified data, credentials, meter configuration, [*internal operating status, log records, firmware*][19]

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 (Application Note 14 from [SM-MSR])

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

[14] [selection: physical, deterministic, hybrid physical, hybrid deterministic]
[15] [assignment: *list of security capabilities*]
[16] [selection: bits, octets of bits, numbers [assignment: *format of the numbers*]]
[17] [assignment: *a defined quality metric*]
[18] [assignment: *access control SFP*]
[19] [assignment: list of subjects and objects, [assignment: *other controlled meter data items*]]

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*[20] to objects based on the following:

(1) Metrologically certified data (e.g., consumption/generation measurements)

(2) Credentials

(3) Meter configuration

(4) [*internal operating status, log records, firmware*][21]

Application Note 15 (Application Note 15 from [SM-MSR])

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: [*an authorised Management Client is allowed to read and write his own Data and log records, Public client is allowed to read basic device information (e.g., SAP, COSEM logical device name, association, frame counter) an authorised Pre-established client is allowed to write unconfirmed application layer objects (e.g., Broadcasting time, image transfer, TOU tables, load control)*][22].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*][23].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*the Public client is not allowed to write any meter data or log records, nobody must be allowed to read the symmetric keys, private keys*][24].

[20] [assignment: *access control SFP*]
[21] [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*]
[22] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[23] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[24] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

Application Note 16 (Application Note 16 from [SM-MSR])

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*[25] on

(1) subjects: all

(2) information: messages

(3) operations: send, receive[26]*.*

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*[27] based on the following types of subject and information security attributes: [

(1) message that be send through local optical port, local RS485, communication module

(2) message that be received through local optical port , local RS485, communication module][28]*.*

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: [

(1) message that be send or received through local optical port, local RS485 will be according to IEC62056-46 standard.

(2) message that be send or received through communication module will be according to IEC62056-47 standard.][29]*.*

[25] [assignment: *information flow control SFP*]
[26] [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*]
[27] [assignment: *information flow control SFP*]
[28] [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]
[29] [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]

FDP_IFF.1.3/Msgs The TSF shall enforce the ***following additional information flow control rules***[30]: [*none*][31].

FDP_IFF.1.4/Msgs The TSF shall explicitly authorise an information flow based on the following rules: [*none*][32].

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) [none][33]

Application Note 17 (Application Note 17 from [SM-MSR])

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).

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.

[30] This refinement is applied to improve readability of the SFR element.
[31] [assignment: *additional information flow control SFP rules*]
[32] [assignment: *rules, based on security attributes, that explicitly authorise information flows*]
[33] [assignment: *other rules, based on security attributes, that explicitly deny information flows*]

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 6.5.1.3 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 6.5.1.3) 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*[34] on
	(1) subjects: all

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

(2) information: all communication[35]

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*[36] based on the following types of subject and information security attributes: [

(1) local optical interface,

(2) local RS485 interface,

(3) communication module interface][37].

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***[38]: [

(1) Meter communication through local optical and RS485 interface will be according to IEC62056-46 standard,

(2) Meter communication through communication module interface will be according to IEC62056-47 standard,

(3) Meter sends out message through P1 interface will be according to IEC62056-21 mode D and DSMR5.0.2 standard

(4) Meter can't receive message through P1 interface][39].

FDP_IFF.1.3/Int The TSF shall enforce the ***following additional information flow control rules***[40]: *None*[41].

FDP_IFF.1.4/Int The TSF shall explicitly authorise an information flow based on the following rules: *None*[42].

---

[35] [assignment: *list of subjects and information*]
[36] [assignment: *information flow control SFP*]
[37] [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]
[38] if the following rules hold
[39] [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]
[40] This refinement is applied to improve readability of the SFR element.
[41] [assignment: *additional information flow control SFP rules*]
[42] [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 [43].

Application Note 18 (Application Note 18 from [SM-MSR])

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*[44] on

(1) subjects: all

(2) information: keys

(3) operations: send, import[45]

[43] [assignment: *rules, based on security attributes, that explicitly deny information flows*]
[44] [assignment: *information flow control SFP*]
[45] [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) – Keys

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*[46] based on the following types of subject and information security attributes: [*shown in the table below*][47].

Table 18 – List of key types

Subject	Information	Security Attribute
TOE, authorised management client;	symmetric keys	symmetric keys according to the security setup (class_id=64) of [B-Book], use the key wrap or key-agreement
	client digital signature public key certificate	client digital signature public key certificate according to the security setup (class_id=64) of [B-Book], use import_certificate;
	client key-agreement public key certificate	client Key-agreement public key certificate according to the security setup (class_id=64) of [B-Book], use import_certificate;
	meter digital signature key pair	meter digital signature key pair according to the security setup (class_id=64) of [B-Book], use generate_key_pair, generate_certificate_request, import_certificate
	meter key-agreement key pair	meter Key-agreement key pair according to the security setup (class_id=64) of [B-Book], use generate_key_pair, generate_certificate_request, import_certificate

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: [

(1) symmetric keys: AES-128 key wrap(confidentiality protection, authentication protection) or key-agreement(confidentiality protection, integrity protection, authentication protection);

(2) client digital signature public key certificate and client Key-agreement public key certificate: import_certificate (confidentiality protection, authentication protection);

(3) meter digital signature key pair and meter Key-agreement key pair: generate_key_pair (Generation of Random Numbers) 、 generate_certificate_request 、 import_certificate(confidentiality protection, integrity protection, authentication protection);][48].

[46] [assignment: *information flow control SFP*]
[47] [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]
[48] [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]

FDP_IFF.1.3/Keys The TSF shall enforce the ***following additional information flow control rules***[49]: [*none*][50].

FDP_IFF.1.4/Keys The TSF shall explicitly authorise an information flow based on the following rules: [*none*] [51].

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) [A key with incorrect type or incorrect length shall be rejected][52].

Application Note 19 (Application Note 19 from [SM-MSR])

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.

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 de-fine unambiguous rules that can therefore be tested (cf. the refinement of ATE_IND.2 in section 6.4.1.7).

[49] This refinement is applied to improve readability of the SFR element.
[50] [assignment: *additional information flow control SFP rules*]
[51] [assignment: *rules, based on security attributes, that explicitly authorise information flows*]
[52] [assignment: *rules, based on security attributes, that explicitly deny information flows*]

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*[53] the following objects: [

(1) dedicated key,

(2) ephemeral keys,

(3) Client Digital signature public key certificate(when no longer needed),

(4) Client Key agreement public key certificate(when no longer needed),

(5) shared secret Z[54]] [55].

Application Note 20 (Application Note 20 from [SM-MSR])

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.

FIA_UAU.6.1 The TSF shall re-authenticate ***authenticate and re-authenticate***[56] the user ***for access to data*** under the conditions defined in the Re-authentication Table[57].

[53] [selection: allocation of the resource to, deallocation of the resource from]
[54] [G-Book]: A shared secret (represented as a byte string) that is used to derive secret keying material using a key derivation method. Source: NIST SP 800-56A Rev. 2: 2013 [NIST SP 800-56A]
[55] [assignment: *list of objects*]
[56] re-authenticate
[57] [assignment: *list of conditions under which re-authentication is required*]

Table 19 – Re-authentication Table

ID	Data	Authentication for initial access	Re-authentication
(1)	*local measurement data*	*Using Security_suite 0*[58] *(AES-GCM-128 for authenticated encryption) during building association and HLS5 GMAC Authentication*	*After a period of 3 min from the previous successful authentication*
(2)	*Configuration data (including the meter time) or other operating parameters.*	*Using Security_suite 0 (AES-GCM-128 for authenticated encryption) during building association and HLS5 GMAC Authentication*	*After a period of 3 min from the previous successful authentication*
(3)	*meter data such as event log and profile data*	*Using Security_suite 0 (AES-GCM-128 for authenticated encryption) during building association and HLS5 GMAC Authentication*	*After a period of 3 min from the previous successful authentication*

Application Note 21 (Application Note 21 from [SM-MSR])

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*[59] ***of*** unsuccessful authentication attempts occur related to *consecutive failed authentication attempts for access to protected data objects*[60].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *surpassed*[61], the TSF shall *block access for that entity via the relevant interface to data requiring prior authentication until the time*

[58] Security suite defined in DLMS/COSEM [B-Book] section 4.4.7 Security setup.
[59] [selection: [assignment: *positive integer number*], an administrator configurable positive integer within [assignment: *range of acceptable values*]]
[60] [assignment: *list of authentication events*]
[61] [selection: met, surpassed]

period shown in the Authentication Failure Handling Table has elapsed[62].

Table 20 – Authentication Failure Handling Table

ID	Type of authentication	Allowed range of authentication failures	Blocked time period
(1)	Association authentication failure	10	*block the user access for 60 minutes and create a log entry into Fraud Detection Log*
(2)	Decryption or authentication failure	10	*block the user access for 60 minutes and create a log entry into Fraud Detection Log*
(3)	Replay attack	10	*block the user access for 60 minutes and create a log entry into Fraud Detection Log*

Application Note 22 (Application Note 22 from [SM-MSR])

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 authentications 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) [Deviation between local time of the TOE and the reliable external time source is too large

(4) TOE hardware / firmware integrity violation or TOE software application integrity violation][63]

6.3.4.2 Tamper notification (FPT_TNN.1)

Tamper notification (FPT_TNN.1)

FPT_TNN.1	*Tamper notification*

[62] [assignment: *list of actions*]
[63] [assignment: *list of types of failures in the TSF*]

Dependencies: None

FPT_TNN.1.1 The TSF shall monitor [magnetic interference, meter cover, terminal cover, module cover] [64] and notify [using remote communication module push alarm to the system administrator by pre-stablished client using Security_suite0 (AES-GCM-128 for authenticated encryption)] [65] when physical tampering of the following types has occurred:

(1) Magnetic interference

(2) [Meter cover removed detection

(3) Terminal cover removed detection][66]

Application Note 23 (Application Note 23 from [SM-MSR])

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 during initial start-up[67] to demonstrate the correct operation of the TSF:

(1) Firmware integrity test

(2) Random bit generator test

(3) Correct TSF start-up

[64] [assignment: *list of TSF devices/elements for which active detection is required*]
[65] [assignment: *designated user(s), role(s), or interface(s)*]
[66] [assignment: *list of additional physical tampering scenarios*]
[67] [selection: during initial start-up (on power on), on reset]

(4) *[All function related parameters and important operation data validity check*

(5) *Physical device interfaces test*

(6) *Test of local communication interface and remote communication module*

(7) *Clock validity test]*[68]

Application Note 24 (Application Note 24 from [SM-MSR])

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

FPT_RPL.1.1 The TSF shall detect replay for the following ***message types*** [69] : [*communicating with the TOE using replay attack message encrypted with the same frame counter*][70].

FPT_RPL.1.2 The TSF shall ~~***perform***~~ [*discard the message and record replay attack error log when it occurs 10 times*][71] 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 (Application Note 25 from [SM-MSR])

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 [*Administrator and* Operator *roles*][72] the ability to query [the currently executing and the most recently downloaded versions of the TOE ***firmware***[73]][74].

---

[68] [assignment: *list of additional self-tests run by the TSF on start-up*]
[69] Refinement of "entities" consistent with section J.8 of [2].
[70] [assignment: *list of identified message types*]
[71] [selection: discard the message, discard the message and [assignment: *list of additional actions*]]
[72] [assignment: *list of authorised roles*]
[73] *software/firmware* – cf. the Glossary definition of firmware applicable in Protection Profile [SM_MSR]
[74] [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 ***firmware***[75] updates to the TOE prior to installing those updates, using a digital signature mechanism that meets the following: [*This process involves encrypted updates, also using the digital signature (ECDSA) to verify the firmware integrity. It's crucial that the firmware update does not affect the stored data, change the device's measuring capabilities, or render the existing driver unsuitable for remote reading operations.*][76]

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: [*after the firmware download successful, then TOE will verify the firmware integrity with the digital signature. The firmware update must only be possible after the authenticity of the firmware update has been verified (using the services of the Security Module and the trust anchor of the Gateway developer) and if the version number of the new firmware is higher to the version of the installed firmware.*][77]

FPT_TSU.1.4 The TSF shall provide *Administrator and* Operator *roles* [78] the ability to activate updates to TOE ***firmware***[79].

Application Note 26 (Application Note 26 from [SM-MSR])

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.

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.

---

[75] *software/firmware* – cf. the Glossary definition of firmware applicable in Protection Profile [SM_MSR]
[76] [assignment: *mechanism specification*]
[77] [assignment: *list of additional properties*]
[78] [assignment: *list of authorised roles*]
[79] *software/firmware* – cf. the Glossary definition of firmware applicable in Protection Profile [SM_MSR]

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[80].

FMT_SMR.1.1 The TSF shall maintain the roles [

(1) authorised Service Technician, Consumer.

(2) authorised meter Administrator, Operator, Reader, Pre-established, Public.][81].

FMT_SMR.1.2 The TSF shall be able to associate ***received messages and keys***[82] with roles.

Application Note 27 (Application Note 27 from [SM-MSR])

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 (Administrator) or maintenance (Operator) 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

FMT_MOF.1.1 The TSF shall restrict the ability to *determine the behaviour of*[83] the functions listed in the *TSF Configuration Table*[84] to the authorised identified roles in the *TSF Configuration Table*[85].

Application Note 28 (Application Note 28 from [SM-MSR])

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

[80] Note that this dependency is not required in this PP because of the refinement in FMT_SMR.1.2 – see section 7.2.2.
[81] [assignment: *the authorised identified roles*]
[82] 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.
[83] [selection: determine the behaviour of, disable, enable, modify the behaviour of]
[84] [assignment: *list of functions*]
[85] [assignment: *the authorised identified roles*]

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.

Table 21 – TSF Configuration Table

ID	Function	Configurable status	Roles Authorised for Configuration
(i)	Allowed number of consecutive failed authentication attempts (FIA_AFL.1)	[Configurable][86]	[*Administrator , Operator*][87]
(ii)	Time period for blocking access after the allowed number of consecutive failed authentication attempts has been exceeded (FIA_AFL.1)	[Configurable][88]	[*Administrator , Operator*][89]
(iii)	Protection level applied to exchange of categories of application data (FDP_IFF.1/Msgs)	[Not configurable][90]	[*None*][91]
(iv)	Triggering of an alarm on the occurrence of an event (FAU_ARP.2)	[Configurable][92]	[*Administrator, Operator*][93]
(v)	Destination of an alarm on the occurrence of an event (FAU_ARP.2)	[Not configurable][94]	[*None*][95]
(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)	[Not configurable][96]	[*None*][97]

Application Note 29 (Application Note 29 from [SM-MSR])

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 configurations 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

[86] [selection, choose one of: Configurable, Not configurable]
[87] [assignment: *the authorised identified roles*]
[88] [selection, choose one of: Configurable, Not configurable]
[89] [assignment: *the authorised identified roles*]
[90] [selection, choose one of: Configurable, Not configurable]
[91] [assignment: *the authorised identified roles*]
[92] [selection, choose one of: Configurable, Not configurable]
[93] [assignment: *the authorised identified roles*]
[94] [selection, choose one of: Configurable, Not configurable]
[95] [assignment: *the authorised identified roles*]
[96] [selection, choose one of: Configurable, Not configurable]
[97] [assignment: *the authorised identified roles*]

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*[98] the *audit log records*[99] to [*authorised Meter Administrator,* Operator][100].

Application Note 30 (Application Note 30 from [SM-MSR])

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*[101] the *meter time*[102] to [*authorised Meter Administrator, Operator, Pre-established*][103].

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*: [*Check in the List of the Event Alarm Table*] [104]

[98] [selection: change_default, query, modify, delete, clear, [assignment: *other operations*]]
[99] [assignment: *list of TSF data*]
[100] [assignment: *the authorised identified roles*]
[101] [selection: change_default, query, modify, delete, clear, [assignment: *other operations*]]
[102] [assignment: *list of TSF data*]
[103] [assignment: *the authorised identified roles*]
[104] [assignment: *list of events and destination for the alarm for each event*]

• *Physical tampering events*: [*Check in the List of the Event Alarm Table*] [105]

• *Other events*: [*Check in the List of the Event Alarm Table*] [106]

Table 22 - List of the Event Alarm Table

Type of Events	List of Events	Destination
Critical events	Clock invalid Battery replace Measurement system error Watchdog error Fraud attempt Total Power Failure Power Resume Missing Neutral	system administrator
Physical tampering events	Magnetic interference, Meter cover removed detection, Module cover removed detection, Terminal cover removed detection,	
Other events	Voltage Missing(aMeter300 only), Voltage Normal, Phase Asymmetry(aMeter300 only), Wrong Phase Sequence(aMeter300 only), Current Reversal, Key Exchanged, Disconnect/Reconnect Failure,	

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: [*None*][107]

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*[108].

Application Note 31 (Application Note 31 from [SM-MSR])

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

[105] [assignment: *list of events and destination for the alarm for each event*]
[106] [assignment: *list of events and destination for the alarm for each event*]
[107] [assignment: *list of alarm messages and associated additional information*]
[108] [assignment: *rules that specify when an alarm must be sent relative to the detection of the event*]

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

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;***~~[109]

b) ~~***All auditable events for the not specified***~~[110] ~~***level of audit; and***~~ [111]

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: [None][112]

(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)

---

[109] In [CC_P2] 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.

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

[111] 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.

[112] [assignment: *list of auditable device error events*]

y) *Security anomaly events as follows:* [*Power Down/up, Clock invalid, Replace Battery /Battery voltage low, Current Reversal, All Events logs in Fraud Detection Log, Disconnect/Reconnect failure*][113]

z) Modification of [*Meter configuration from FDP_ACF.1*][114]

aa) Self-test completed [FPT_BST.1]

bb) [*None*][115].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

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*;
- [*None*][116].

Application Note 32 (Application Note 32 from [SM-MSR])

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.

Application Note from the ST author 1

[113] [assignment: *list of auditable security anomaly events*]
[114] [assignment: *list of specified auditable data categories*]
[115] [assignment: *other specifically defined auditable events*]
[116] [assignment: *other audit relevant information*]

The following events cannot be found directly in the event logs, or missing:

- **Change in network status**: Event ID 76-87 in Power quality event log, the supply power network missing voltage, under voltage, over voltage and return to normal.
- **Energy supply connect/disconnect:** Event ID 59-69 in Disconnector control log
- **Load limitation configuration/activation**: Event ID 65, 66, 67 in Disconnector control log
- **Key generation**: Event ID 48(Global key(s) changed) in standard event log
- **Message received from an unauthorised source**: All unauthorised source communication to TOE will record event ID 46, 49, 50 in fraud detection log.
- **Key received from an unauthorised source**: All unauthorised source communication to TOE will record event ID 46, 49, 50 in fraud detection log.
- **Change of access rights**: The access rights cannot to be change.
- **Random bit generator test**: Events will be recorded when a fault occurs during test the random bit generator, event ID 250 (Random bit generator failed).
- **Correct TSF start-up**: Event ID 2(Power up) in standard event log, the power up event log is recorded after all TSF start-up correctly.
- **Failure of the random bit generator**: Event ID 250(Random bit generator failed) in standard event log
- **Self-test completed**: Event ID 2(Power up) in standard event log, the self-test during the system start-up process is completed before recording the power up event log, and the periodically self-test during normal operation will not record event log except occur any of failure.

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 [*Meter Administrator,* Operator*, Reader*][117] with the capability to read *the contents*[118] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in **the format specific in the following reference: [**

(1) DLMS UA 1000-1 Ed 15 [B-Book],

(2) DLMS UA 1000-2 Ed. 11 [G-Book],

(3) IDIS Package 2, IP Profile Ed.2.0 [IDIS-ID],

(4) IDIS Package 2, Smart metering Objects, Ed.2.0[IDIS-SM]][119].

Application Note 33 (Application Note 33 from [SM-MSR])

[117] [assignment: *authorised users*]
[118] [assignment: *list of audit information*]
[119] 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. [assignment: *document reference details]*

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

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 [use a Client that have read-access]***[120].

Table 23 - Client Access table

Client	Client SAP	Behavior
Administrator	1	· Read all data · Configure all parameters · Method all
Operator	111	· Read all data · Configure all parameters · Method all
Reader	112	· Read all data
Pre-established	102	· Configure partial parameters · Method partial · Push
Public	16	·Read partial data (COSEM logic name, Billing period counter, Security Receive frame counter, Association, SAP Assignment)

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*[121] ~~***unauthorised***~~[122] modifications to the stored audit records in the audit trail.

Application Note 34 (Application Note 34 from [SM-MSR])

[120] 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. [assignment: *description of method for assigning access*]

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

[122] 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.

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*[123] if the audit trail exceeds: [*In the Logbooks Capacity Table*] [124]

Table 24 - The Logbooks Capacity Table

Logbooks	Capacity(Entries)
Standard Event Log	500
Fraud Detection Log	200
Communication log	200
Disconnector Control log	200
Power Quality log	200
Power Failure Management	200

Application Note 35 (Application Note 35 from [SM-MSR])

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 TOE Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL3+ augmented with ALC_FLR.3.

Table 25 – Security Assurance Requirements

Assurance Requirements		
Class ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Class ALC: Life Cycle Support	ALC_CMC.3	Authorisation controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.3	Systematic flaw remediation

[123] [assignment: *actions to be taken in case of possible audit storage failure*]
[124] [assignment: *pre-defined limit* ***in terms of number of records supported***]

	ALC_LCD.1	Developer defined life-cycle model
Class ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design
Class AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Class ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

6.4.1 Refinements of Security Assurance Requirements

The following refinements are made to selected assurance requirements in Table 25 – Security Assurance Requirements.

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 19).

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[125]:
   - 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

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

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 19). 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
    - 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).
17. 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)

6.5 Security Requirements Rationale

6.5.1 Security Requirements Coverage

The Table 26 - Security Functional Requirements Related to Security Objectives in section 6.5.1.1 provides a mapping between the Security Functional Requirements and the Security Objectives, illustrating that each Security Functional Requirement covers at least one Objective and that each Objective is covered by at least one Security Functional Requirement.

6.5.1.1 Security Functional Requirements Related to Security Objectives

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

Table 26 - Security Functional Requirements Related to Security Objectives

	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								

	O.Authorisation	O.Messages	O.DataAtRest	O.Crypto	O.Interfaces	O.Resilience	O.SecureUpdate	O.Logging	O.Alarms
FCS_CKM.1		X		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		
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	

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:

- The iterations of FCS_COP.1 describe the 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:

- The iterations of FCS_COP.1 describe the 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
- The iterations of FCS_COP.1 specify 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.

6.5.1.2 Security Assurance Requirements Rationale

The assurance level for this security target 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 [CC_P3] 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.

6.6 Requirements Dependency Rationale

6.6.1 Rationale Showing that Dependencies are Satisfied

The SFRs in this ST satisfy all the required dependencies listed in the Common Criteria. The table in this section lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As it is indicated by the table, all dependencies are fulfilled.

6.6.1.1 Security Functional Requirements Dependencies

The following table provides a summary of the SFRs and their dependencies

Table 27 - Summary of Security Functional Requirements Dependencies

Requirement	Dependencies	Fulfilled by
FCS_CKM.1	[FCS_CKM.2 or	FCS_COP.1

Requirement	Dependencies	Fulfilled by
	FCS_COP.1] FCS_CKM.4	FCS_CKM.4 See also note below on distribution of keys generated in the meter
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
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_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).

Requirement	Dependencies	Fulfilled by
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 13 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.
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

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 [CC_P2]), 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 12 (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.

6.6.1.2 Security Assurance Requirements Dependencies

The following table provides a summary of the SARs and their dependencies.

Table 28 - SAR Dependencies

Component	Depends On:	Which is:
ADV_ARC.1	ADV_FSP.1	hierarchically higher component ADV_FSP.3 is included.
	ADV_TDS.1	hierarchically higher component ADV_TDS.2 is included.
ADV_FSP.3	ADV_TDS.1	hierarchically higher component ADV_TDS.2 is included.
ADV_TDS.2	ADV_FSP.3	included
AGD_OPE.1	ADV_FSP.1	hierarchically higher component ADV_FSP.3 is included.
AGD_PRE.1	no dependencies	not applicable
ALC_CMC.3	ALC_CMS.1	hierarchically higher component ALC_CMS.3 is included.
	ALC_DVS.1	included
	ALC_LCD.1	included
ALC_CMS.3	no dependencies	not applicable
ALC_DEL.1	no dependencies	not applicable
ALC_DVS.1	no dependencies	not applicable
ALC_LCD.1	no dependencies	not applicable
ALC_FLR.3	no dependencies	not applicable
ASE_CCL.1	ASE_ECD.1	included
	ASE_INT.1	included
	ASE_REQ.1	hierarchically higher component ASE_REQ.2 is included
ASE_ECD.1	no dependencies	not applicable
ASE_INT.1	no dependencies	not applicable
ASE_OBJ.2	ASE_SPD.1	included
ASE_REQ.2	ASE_ECD.1	included
	ASE_OBJ.2	included
ASE_SPD.1	no dependencies	not applicable
ASE_TSS.1	ADV_FSP.1	hierarchically higher component ADV_FSP.3 is included
	ASE_INT.1	included
	ASE_REQ.1	hierarchically higher component ASE_REQ.2 is included
ATE_COV.2	ADV_FSP.2	hierarchically higher component ADV_FSP.3 is included
	ATE_FUN.1	included
ATE_DPT.1	ADV_ARC.1	included
	ADV_TDS.2	included
	ATE_FUN.1	included
ATE_FUN.1	ATE_COV.1	hierarchically higher component ATE_COV.2 is included

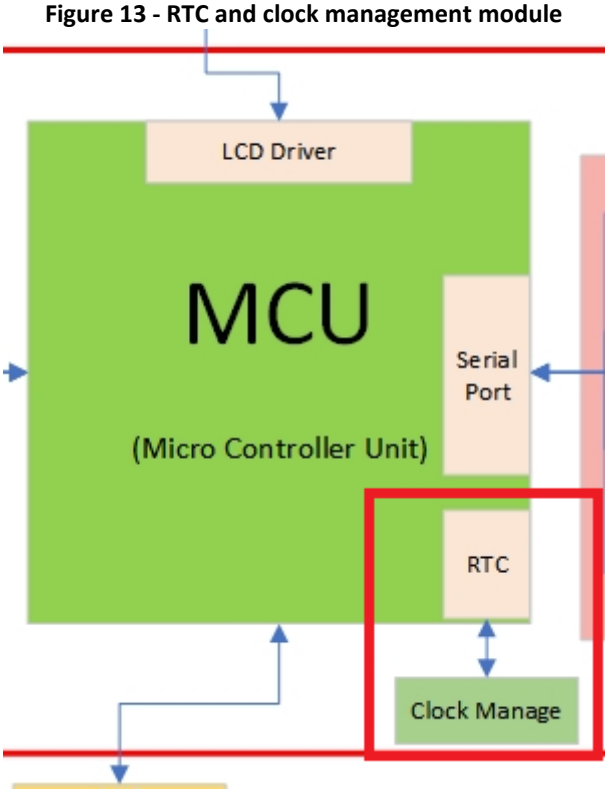
Component	Depends On:	Which is:
ATE_IND.2	ADV_FSP.2	hierarchically higher component ADV_FSP.3 is included
	AGD_OPE.1	included
	AGD_PRE.1	included
	ATE_COV.1	hierarchically higher component ATE_COV.2 is included
	ATE_FUN.1	included
AVA_VAN.2	ADV_ARC.1	included
	ADV_FSP.2	hierarchically higher component ADV_FSP.3 is included
	ADV_TDS.1	included
	AGD_OPE.1	included
	AGD_PRE.1	included

7 TOE Summary Specification

7.1 Real-Time Clock

The meter equipped a RTC module, the module will manage the whole time.

Figure 13 - RTC and clock management module



7.1.1 Calendar

- Support for automatic conversion of calendar, timing, and leap year.
- MCU has built-in real-time clock module, which uses 32768Hz crystal oscillator as clock source to calculate.
- The accuracy of the clock can reach 0.5 s/d at 25 ℃ after modification.

- Independent power supply to The RTC module. It is powered from the main supply in normal operation mode and powered by battery during power failure period.

Table 29 - Clock Range

Year	Month	Day	Week	Hour	Minute	Second
2000~2099	1~12	1~31	1(Mon.)~7(Sun.)	0~23	0~59	0~59

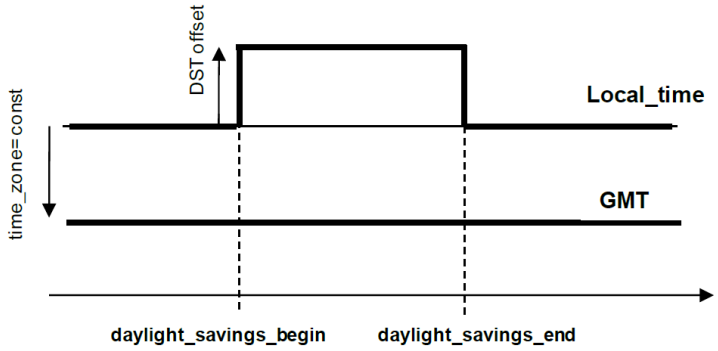
- The following instances allow the management

Table 30 - Managed instances

Item	Class	OBIS
Clock	Class Id 8	Logical name 0-0:1.0.0.255

7.1.2 Daylight Saving Time

Figure 14 - DTS



time_zone: attribute 3 of IC Clock in minutes. It is a constant depending on the geographic location (example: Paris: -60 minutes)

deviation: part of type “date_time” in minutes. Is dynamic and changes depending on the time_zone and if DST is active or not. It is calculated by the server

Local_time: local time (current time)

DST offset: Daylight saving time offset in minutes (“summer time” – “winter time”)

UTC: Greenwich Mean Time

Deviation = UTC - Local_time

Deviation = time_zone – DST offset (if DST is active)

When the meter clock is set with DST flag, the 0xFF of DST status undefined is always supported on meter.

Table 31 - DTS deviation

Year, month, day of month, day of week, hour, minute, second, hundredths of seconds	deviation	Clock status	Supported by the meter
the meter's local time	0x8000 (not specified)	DST undefined: 0xFF	mandatory
the meter's local time	0x8000 (not specified)	DST defined: 0x80/0x00	optional
local (undefined location) time	Deviation of the given (transmitted) local time to UTC	DST not active: 0x00	optional

- Daylight savings begin: set
- Daylight savings end: set
- Daylight savings deviation: -120…120 min
- Daylight savings enabled: set
- Remarks:
    1. The time of the event recording is the time adjusted by the summertime.
    2. Daylight saving time priority: DST > demand > rate > Load > rate activation > settlement
    3. When the demand generation point coincides with the summertime, the current maximum demand rate is the time adjusted by the summertime.
    4. The time formatting rules of IDIS, reference IDIS pack2 6.6.

7.2 Event Log

7.2.1 General Information

The capacity of the audit trail can be found in Table 24 - The Logbooks Capacity Table.

The following objects allow the management some events and record corresponding information:

Table 32 - Events and records

Event/Record	Class id	Logical name
Time threshold for long power failures	Class Id 3	Logical name 0-0:96.7.20.255
Number of power failures in any phase	Class Id 1	Logical name 0-0:96.7.21.255
Number of long power failures in any phase	Class Id 1	Logical name 0-0:96.7.9.255
Duration of the last power failure in any phase	Class Id 3	Logical name 0-0:96.7.19.255
Threshold for voltage sag	Class Id 3	Logical name 1-0:12.31.0.255
Time threshold for voltage sag	Class Id 3	Logical name 1-0:12.43.0.255
Number of voltage sag on L1	Class Id 1	Logical name 1-0:32.32.0.255
Number of voltage sag on L2	Class Id 1	Logical name 1-0:52.32.0.255
Number of voltage sag on L3	Class Id 1	Logical name 1-0:72.32.0.255
Duration of last voltage sag on L1	Class Id 3	Logical name 1-0:32.33.0.255
Duration of last voltage sag on L2	Class Id 3	Logical name 1-0:52.33.0.255
Duration of last voltage sag on L3	Class Id 3	Logical name 1-0:72.33.0.255
Magnitude of the last voltage sag on L1	Class Id 3	Logical name 1-0:32.34.0.255
Magnitude of the last voltage sag on L2	Class Id 3	Logical name 1-0:52.34.0.255
Magnitude of the last voltage sag on L3	Class Id 3	Logical name 1-0:72.34.0.255
Threshold for voltage swell	Class Id 3	Logical name 1-0:12.35.0.255

Time threshold for voltage swell	Class Id 3	Logical name 1-0:12.44.0.255
Number of voltage swell on L1	Class Id 1	Logical name 1-0:32.36.0.255
Number of voltage swell on L2	Class Id 1	Logical name 1-0:52.36.0.255
Number of voltage swell on L3	Class Id 1	Logical name 1-0:72.36.0.255
Duration of last voltage swell on L1	Class Id 3	Logical name 1-0:32.37.0.255
Duration of last voltage swell on L2	Class Id 3	Logical name 1-0:52.37.0.255
Duration of last voltage swell on L3	Class Id 3	Logical name 1-0:72.37.0.255
Magnitude of the last voltage swell on L1	Class Id 3	Logical name 1-0:32.38.0.255
Magnitude of the last voltage swell on L2	Class Id 3	Logical name 1-0:52.38.0.255
Magnitude of the last voltage swell on L3	Class Id 3	Logical name 1-0:72.38.0.255
Threshold for missing voltage(voltage cut)	Class Id 3	Logical name 1-0:12.39.0.255
Time threshold for voltage cut	Class Id 3	Logical name 1-0:12.45.0.255
Threshold of Unbalance Current L0(neutral > live line)	Class Id 3	Logical name 1-0:31.39.0.255
Current unbalance time threshold	Class Id 3	Logical name 1-0:31.45.0.255
Event object - standard event log	Class Id 7	0-0:96.11.0.255
Event object - fraud detection log	Class Id 7	0-0:96.11.1.255
Event object - communication log	Class Id 7	0-0:96.11.5.255
Event object - disconnector control log	Class Id 7	0-0:96.11.2.255
Event object - power quality log	Class Id 7	0-0:96.11.4.255

7.2.2 Standard Event Log

The standard logbook records the occurrence of the events:

Table 33 - Standard event log

Event Id	Event Name	Description
1	Power Down	Indicates a complete power down of the device. Please note that this is related to the device and not necessarily to the network.
2	Power Up	Indicates that the device is powered again after a complete power down.
3	Daylight saving time enabled or disabled	Indicates the regular change from and to daylight saving time. The time stamp shows the time before the change. This event is not set in case of manual clock changes and in case of power failures.
4	Clock adjusted (old date/time)	Indicates that the clock has been adjusted. The date/time that is stored in the event log is the old date/time before adjusting the clock.
5	Clock adjusted (new date/time)	Indicates that the clock has been adjusted. The date/time that is stored in the event log is the new date/time after adjusting the clock.
6	Clock invalid	Indicates that clock may be invalid, i.e. if the power reserve of the clock has exhausted. It is set at power up.
7	Replace Battery	Indicates that the battery must be exchanged due to the expected end of life time. The threshold is 2.9V.
8	Battery voltage low	Indicates that the current battery voltage is low. The threshold is 2.9V, ignore interval 60s.
9	TOU activated	Indicates that the passive TOU has been activated.
10	Error register cleared	Indicates that the error register was cleared.
11	Alarm register cleared	Indicates that the alarm register was cleared.

12	Program memory error	Indicates a physical or a logical error in the program memory.
13	RAM error	Indicates a physical or a logical error in the RAM.
14	NV memory error	Indicates a physical or a logical error in the non-volatile memory
15	Watchdog error	Indicates a watch dog reset or a hardware reset of the microcontroller.
16	Measurement system error	Indicates a logical or physical error in the measurement system
17	Firmware ready for activation	Indicates that the new firmware has been successfully downloaded and verified, i.e. it is ready for activation
18	Firmware activated	Indicates that a new firmware has been activated
19	Passive TOU programmed	The passive structures of TOU or a new activation date/time were programed
47	One or more parameters changed	Indicates the change of at least one parameter
48	Global key(s) changed	One or more global keys changed, now just for BK and EK
51	FW verification failed	Indicates the transferred firmware verification failed i.e. cannot be activated.
88	Phase sequence reversal	Indicates wrong mains connection. Usually indicates fraud or wrong installation. For poly phase connection only!
89	Missing neutral	Indicates that the neutral connection from the supplier to the meter is interrupted . For single phase meter,condition is that current of Line is more 5%Ib and current of neutral is lower than 1%Ib, ignore interval 30s. For three phase meter,(Vmax-Vmin)/Vmax > threshold)(default 30%), ignore interval 30s.
250	Random bit generator failed	Indicates the random bit generator output random bit data failed.
254	Load profile cleared	Any of the profiles cleared. NOTE: If it appears in Standard Event Log then any of the E-load profiles was cleared. If the event appears in the M-Bus Event log then one of the M-Bus load profiles was cleared
255	Event log cleared	Indicates that the event log was cleared. This is always the first entry in an event log. It is only stored in the affected event log.

- The following objects related to standard logbook ：

Standard event logbook	Class Id 7	Logical name 0-0:99.98.0.255

- The standard logbook is as defined below:

Minimum capacity	500 entries minimum			
Capture objects	Clock	8	0-0:1.0.0.255	2
	Standard event object	1	0-0:96.11.0.255	2
Capture period	Asynchronous			
Buffer encoding	According to IDIS normal			
Selective access	According to IDIS: by date			

Sort method	Sorted by the smallest with sort object set to the clock attribute 2 or unsorted (FIFO)
Methods	
Reset	0

7.2.3 Fraud Detection Log

The fraud logbook shall record the occurrence of the events.

Table 34 - Fraud detection logs

Event Id	Event Name	Description
40	Terminal cover removed	Indicates that the terminal cover has been removed. 1 second ignore interval.
41	Terminal cover closed	Indicates that the terminal cover has been closed. 1 second ignore interval.
42	Strong DC field detected	Indicates that a strong magnetic DC field has been detected. 1 second ignore interval.
43	No strong DC field anymore	Indicates that the strong magnetic DC field has disappeared. 1 second ignore interval.
44	Meter cover removed	Indicates that the meter cover has been removed. 1 second ignore interval.
45	Meter cover closed	Indicates that the meter cover has been closed. 1 second ignore interval.
46	Association authentication failure (n time failed authentication)	Indicates that a user tried to gain LLS access with wrong password (intrusion detection) or HLS access challenge processing failed n-times
49	Decryption or authentication failure (n time failure)	Decryption with currently valid key (global or dedicated) failed to generate a valid APDU or authentication tag
50	Replay attack	Receive frame counter value less or equal to the last successfully received frame counter in the received APDU Event signalizes as well the situation when the DC has lost the frame counter synchronization.
384	Module cover removed	Indicates that the Module cover has been removed. 1 second ignore interval.
385	Module cover closed	Indicates that the Module cover has been closed. 1 second ignore interval.
255	Event log cleared	Indicates that the event log was cleared. This is always the first entry in an event log. It is only stored in the affected event log.

Note: In the case the meter cover cannot be removed, the Event Id 44 and 45 may not be supported.

- The following objects related to standard logbook：

Fraud Detection event logbook	Class Id 7	Logical name 0-0:99.98.1.255

- The fraud logbook is defined as below

Minimum capacity	200 entries minimum			
Capture objects	Clock	8	0-0:1.0.0.255	2
	Fraud event object	1	0-0:96.11.1.255	2
Capture period	Asynchronous			
Buffer encoding	According to IDIS normal			

Selective access	According to IDIS: by date
Sort method	Sorted by the smallest with sort object set to the clock attribute 2 or unsorted (FIFO)
Methods	
Reset	0

7.2.4 Communication Log

The communication logbook shall record the occurrence of the events.

Table 35 - Communication logs

Event Id	Event Name	Description
245	485 connected	Indicates a successful communication on 485 port has been initiated.
246	IR connected	Indicates a successful communication on IR port has been initiated.
247	GPRS connected	Indicates a successful communication on GPRS local port has been initiated.
255	Event log cleared	Indicates that the event log was cleared. This is always the first entry in an event log. It is only stored in the affected event log.

- The following objects related to standard logbook ：

Communication event logbook	Class Id 7	Logical name 0-0:99.98.5.255

- The communication logbook is defined as below:

Minimum capacity	200 entries minimum			
Capture objects	Clock	8	0-0:1.0.0.255	2
	Communication event object	1	0-0:96.11.5.255	2
Capture period	Asynchronous			
Buffer encoding	According to IDIS normal			
Selective access	According to IDIS: by date			
Sort method	Sorted by the smallest with sort object set to the clock attribute 2 or unsorted (FIFO)			
Methods				
Reset	0			

7.2.5 Disconnector Control Log

The following events are recorded in the disconnector logbook:

Table 36 - Disconnector control log

Event Id	Event name	Description
59	Disconnector ready for manual reconnection	Indicates that the disconnector has been set into the Ready_for_reconnection state and can be manually reconnected
60	Manual disconnection	Indicates that the disconnector has been manually disconnected
61	Manual connection	Indicates that the disconnector has been manually connected.
62	Remote disconnection	Indicates that the disconnector has been remotely disconnected.

63	Remote connection	Indicates that the disconnector has been remotely connected.
64	Local disconnection	Indicates that the disconnector has been locally disconnected (i.e. via the limiter or current supervision monitors).
65	Limiter threshold exceeded	Indicates that the limiter threshold has been exceeded.
66	Limiter threshold ok	Indicates that the monitored value of the limiter dropped below the threshold.
67	Limiter threshold changed	Indicates that the limiter threshold has been changed
68	Disconnect/Reconnect failure	Indicates that a failure of disconnection or reconnection has happened (control state does not match output state)
69	Local reconnection	Indicates that the disconnector has been locally re-connected (i.e. via the limiter or current supervision monitors).
70	Supervision monitor 1 threshold exceeded	Indicates that the supervision monitor threshold has been exceeded.
71	Supervision monitor 1 threshold ok	Indicates that the monitored value dropped below the threshold.
72	Supervision monitor 2 threshold exceeded	Indicates that the supervision monitor threshold has been exceeded.
73	Supervision monitor 2 threshold ok	Indicates that the monitored value dropped below the threshold.
74	Supervision monitor 3 threshold exceeded	Indicates that the supervision monitor threshold has been exceeded.
75	Supervision monitor 3 threshold ok	Indicates that the monitored value dropped below the threshold.
255	Event log cleared	Indicates that the event log was cleared. This is always the first entry in an event log. It is only stored in the affected event log

- The following objects related to standard logbook:

Disconnector control event logbook	Class Id 7	Logical name 0-0:99.98.2.255

- The disconnector logbook is defined as below:

Minimum capacity	200 entries minimum			
Capture objects	Clock	8	0-0:1.0.0.255	2
	Disconnector event object	1	0-0:96.11.2.255	2
	Limiter threshold	71	0-0:17:0.0.255	3
Capture period	Asynchronous			
Buffer encoding	According to IDIS normal			
Selective access	According to IDIS: by date			
Sort method	Sorted by the smallest with sort object set to the clock attribute 2 or unsorted (FIFO)			
Methods				
Reset	0			

7.2.6 Power Quality Log

The power quality logbook records the events.

Table 37 - Power Quality Log

Event Id	Event Name	Description
76	Undervoltage L1	Indicates undervoltage on at least L1 phase was detected.
77	Undervoltage L2	Indicates undervoltage on at least L2 phase was detected.
78	Undervoltage L3	Indicates undervoltage on at least L3 phase was detected.
79	Overvoltage L1	Indicates overvoltage on at least L1 phase was detected.
80	Overvoltage L2	Indicates overvoltage on at least L2 phase was detected.
81	Overvoltage L3	Indicates overvoltage on at least L3 phase was detected.
82	Missing voltage L1	Indicates that the voltage on at least L1 phase has fallen below the Umin threshold for longer than the time delay.
83	Missing voltage L2	Indicates that the voltage on at least L2 phase has fallen below the Umin threshold for longer than the time delay.
84	Missing voltage L3	Indicates that the voltage on at least L3 phase has fallen below the Umin threshold for longer than the time delay.
85	Voltage L1 normal	Indicates that the mains voltage is in normal limits again, e.g. after overvoltage.
86	Voltage L2 normal	Indicates that the mains voltage is in normal limits again, e.g. after overvoltage.
87	Voltage L3 normal	Indicates that the mains voltage is in normal limits again, e.g. after overvoltage.
90	Phase Asymmetry	Indicates phase asymmetry due to large unbalance of loads connected
91	Current reversal	Indicates unexpected energy export (for devices which are configured for energy import measurement only)
255	Event log cleared	Indicates that the event log was cleared. This is always the first entry in an event log. It is only stored in the affected event log.

- The following objects related to standard logbook:

Power quality logbook	Class Id 7	Logical name 0-0:99.98.4.255

- The power quality logbook is defined as below:

Minimum capacity	200 entries minimum			
Capture objects	Clock	8	0-0:1.0.0.255	2
	Power quality event	1	0-0:96.11.8.255	2
Capture period	Asynchronous			
Buffer encoding	According to IDIS normal			
Selective access	According to IDIS: by date			
Sort method	Sorted by the smallest with sort object set to the clock attribute 2 or unsorted (FIFO)			
Methods				
Reset	0			

7.2.7 Power Failure Management

The following objects related to power failure management:

Power failure event logbook	Class Id 7	Logical name 1-0:99.97.0.255

Note: The type of the attribute 2 of the duration of the last power failure in any phase must be a double long unsigned and NOT a long unsigned.

The power failure logbook records the power failures in all phases and their duration. Electricity metering devices shall implement the power failure logbook.

Minimum capacity	200 entries			
Capture objects	Clock	8	0-0:1.0.0.255	2
	PF duration	3	0-0:96.7.19.255	2
Capture period	Asynchronous			
Buffer encoding	According to IDIS: normal or compressed			
Selective access	By range (from date to date)			
Sort method	Sorted by the smallest with sort object set to the clock attribute 2 or unsorted (FIFO)			
Methods				
Reset	0			

7.3 Security

7.3.1 General

The Meter support one security contexts. The security context is configured by its security setup object. In this security setup object, the global unicast key is related to the "Administrator/Operator/Reader Client association". The attributes "security_suite" can be programmed. If "security_ suite" set to 0, then AES-GCM-128 authenticated encryption and AES-128 key wrap will be supported, if "security_ suite" set to 1, then AES-GCM-128 authenticated encryption, ECDSA P-256 digital signature, ECDH P-256 key agreement, SHA-256 hash and AES-128 key wrap will be supported.

The TOE uses Security_suite 0 (AES-GCM-128 for authenticated encryption) during building association and HLS5 GMAC Authentication, and requires a re-authentication when after a period of 3 min from the previous successful authentication.

After several unsuccessful authentication attempts occur the access to protected data objects will be blocked, for details see Table 20 – Authentication Failure Handling Table.

To protect the TOE from replay attack, each APDU of communication message carries a frame counter, and every APDU should have a higher frame counter than the previously received one. In addition, the frame counter also participates in the encryption operation of the current APDU. If the frame counter is incorrect, it will cause the decryption of the encrypted APDU to fail. Messages with invalid frame counter are dropped without processing, the communication port will be locked if number of consecutive frame counter invalid. So this can protect the TOE from replay attack.

Table 38 - Clients

Client	Client SAP	Behavior	Services supported by a Server

Administrator	1	Read all data Configure all parameters Method all	· Block-transfer-with-get · Block-transfer-with-set · Get · Set · Multiple-references · Selective Access · Action · General-block-transfer · General-protection
Operator	111	Read all data Configure all parameters Method all	· Block-transfer-with-get · Block-transfer-with-set · Get · Set · Multiple-references · Selective Access · Action · General-block-transfer · General-protection
Reader	112	Read all data	· Block-transfer-with-get · Block-transfer-with-set · Get · Set · Multiple-references · Selective Access · Action · General-block-transfer · General-protection
Pre-established	102	Configure partial parameters Method partial Push	· Set · Action · Data-Notification · General-block-transfer · General-protection
Public	16	Read partial data(COSEM logic name, Billing period counter, Security Receive frame counter, Association, SAP Assignment)	· Block-transfer-with-get · Get

In addition to these, only the Administrator and Operator roles can delete the event logs, so no unauthorized deletion is possible. Also, only these two roles have the rights to modify the meter clock.

Table 39 Client Name match to OBIS

Client name	Association(Classs id 15)	Security Setup (Classs id 64)	Frame counter
Administrator	0-0:40.0.3.255	0-0:43.0.0.255	0-0:43.1.0.255
Operator	0-0:40.0.5.255	0-0:43.0.1.255	0-0:43.1.3.255
Reader	0-0:40.0.4.255	0-0:43.0.2.255	0-0:43.1.2.255

Pre-established	0-0:40.0.2.255	0-0:43.0.0.255	0-0:43.1.1.255
Public	0-0:40.0.1.255	NA	NA

These roles are available on the Communication Module, the Optical Interface, and the RS-485. As the P1 Interface is only capable of sending public information for a IHD it does not require roles and access rights. The DLMS object model [DLMS_OLIST] contains information about the available security functionality (objects) and its attributes. The cellular and optical interfaces are available for every user, but the object model will define the available functionality for every user role.

The DLMS/COSEM model was designed to meet the increasing business needs for meters to be not only a simple date recording device but be a utility meter which is part of an integrated metering, control, and billing system.

COSEM, the *Companion Specification for Energy Metering*, addresses these challenges by looking at the utility meter as part of a complex measurement and control system. The meter has to be able to convey measurement results from the metering points to the business processes which use them. It also has to be able to provide information to the consumer and manage consumption and eventually local generation.

COSEM achieves this by using object modelling techniques to model all functions of the meter, without making any assumptions about which functions need to be supported, how those functions are implemented and how the data are transported. The formal specification of COSEM interface classes forms a major part of COSEM.

To process and manage the information it is necessary to uniquely identify all data items in a manufacturer-independent way. The definition of OBIS, the Object Identification System is another essential part of COSEM. It is based on *DIN 43863-3:1997, Electricity meters – Part 3: Tariff metering device as additional equipment for electricity meters – EDIS – Energy Data Identification System* [DIN 43863-3]. The set of OBIS codes has been considerably extended over the years to meet new needs.

COSEM models the utility meter as a server application used by client applications that retrieve data from, provide control information to, and instigate known actions within the meter via controlled access to the COSEM objects. The clients act as agents for third parties i.e., the business processes of energy market participants.

The standardized COSEM interface classes form an extensible library. Manufacturers use elements of this library to design their products that meet a wide variety of requirements.

The server offers means to retrieve the functions supported, i.e., the COSEM objects instantiated. The objects can be organized to logical devices and application associations and to provide specific access rights to various clients. [B-Book]

[DLMS_OLIST] contains all the relevant COSEM objects according to the TOE. Every object has its own attributes defined in the [B-Book]. The object model indicates the available operations

for every object and attribute to every user role (Access rights). There are 3 operations connected to the objects' attributes and access rights:

- GET: read the attribute
- SET: set/modify the attribute
- ACTION: perform an action, e.g., the relay object can be connected or disconnected remotely.

The COSEM object model is stored in the code flash of the TOE. The object model is defined as read-only data in the firmware, and the modification of the object model is only available through a firmware upgrade.

As the role model and the objects with their attributes are handled in the DLMS/COSEM model [DLMS_OLIST], after a user is authenticated by the TOE, in the parameterization tool (Meter Parameter Management System – MPMS, version: V1.0.9.hu) only those objects will be available for which the user has access to. The TOE input validation is handled by the MPMS and warns the user about it. If in any case the TOE receives an incorrect value for an attribute it drops the message without a warning.

In case of an operational error or failure, there is no user operation to be done. Every process following a failure will be done automatically.

7.3.2 Objects

The following objects are mandatory for the registration use case

Security Setup - Administrator	Class Id 64	0-0:43.0.0.255
Security Setup - Operator	Class Id 64	0-0:43.0.1.255
Security Setup - Reader	Class Id 64	0-0:43.0.2.255
Public association	Class Id 15	0-0:40.0.1.255
Administrator association	Class Id 15	0-0:40.0.3.255
Operator association	Class Id 15	0-0:40.0.5.255
Reader association	Class Id 15	0-0:40.0.4.255
Security - Receive frame counter - broadcast key	Class Id 1	0-0:43.1.1.255
Security - Receive frame counter - unicast key	Class Id 1	0-0:43.1.0.255
Security - Receive frame counter - unicast key - Reader	Class Id 1	0-0:43.1.2.255
Security - Receive frame counter - unicast key - Operator	Class Id 1	0-0:43.1.3.255

Security_suite

(0) AES-GCM-128 for authenticated encryption and AES-128 for key wrapping
(1) AES-GCM-128 authenticated encryption, ECDSA P-256 digital signature, ECDH P-256 key agreement, SHA-256 hash and AES-128 key wrapping.

7.3.3 Default Global Keys for Interoperability Testing

For testing purposes, the following default security material should be used:

Table 40 - Default values for interoperability testing

Security Parameter	Default value(hex)
Global Authenticate key	0xD0 D1 D2 D3 D4 D5 D6 D7 D8 D9 DA DB DC DD DE DF
Global Broadcast key	0x0F 0E 0D 0C 0B 0A 09 08 07 06 05 04 03 02 01 00
Global Encryption key	0x00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

Master key	0X00 11 22 33 44 55 66 77 88 99 AA BB CC DD

7.3.4 Tamper protection

Tamper detection includes Meter cover removed, Terminal cover removed, Strong DC magnetic field, the hardware (electronic circuit) is equipped with relevant sensors.

When a tamper detected, a tamper event will be recorded in the Fraud Detection Log with the corresponding event code and time stamp, the details of fraud detection log is in the section 7.2.3. At the same time, will push alarm to the system administrator via the module if the push alarm filter register is enabled, the details of push alarm is in the section 7.4.5.

7.3.5 Self-protection

7.3.5.1 Self-tests

The TOE implements several self-tests which will execute at system startup and on request by Service Technician/Consumer and periodically during normal operation. The tests contain:

1. Integrity check of all function related parameters and the important operation data. There is a CRC[126] include to every function related parameter or operation data, if the CRC which calculating from current data is not match to the original CRC, it can be consider as a data incomplete.
2. Operation status of physical device interfaces, such as relay, button, battery voltage. A failure case will be considered if the status of physical device interfaces is different from their expect status.
3. Operation status of local communication interface and remote communication module. Abnormal working state will be considered if the communication interface no receive/send data in a time that exceed the time threshold.
4. The clock is running on the RTC module of MCU. The validity check of the clock is performed during the power on initialization process and normal operation power supply by grid, when there is a power outage in the grid, it is kept by super capacitors and battery. MCU can recognize whether the clock is valid or not by judge the range of Year, Month, Day, Hour, Minute, and Second values(e.g. month>12, day>31, hour>23), this will trigger push a clock error message, then the responsible administrator or service provider will send a clock synchronization command to TOE to correct it.
5. Integrity of firmware check perform when the meter powered on, the bootload program calculates the CRC32 of the app firmware (Except the first 4 bytes), compares this CRC32 with the first 4 bytes of the firmware. If the comparison is successful, runs this part app program. If the comparison fails, repeat the calculation and comparison until the comparison is successful.
6. TOE uses the MCU's built-in hardware random bit generator, it will be check during the power on initialization process and every time it needs to be used for communication. A failure case will be considered if the generation completion bit of the hardware

[126] The CRC-16-CCITT (using the polynomial: X16+X12+X5+1, uses XOR in, XOR out and is computed with least significant bit first) is used. It is same as the verification algorithm of frame checksum of HDLC protocol. It is only used to check the integrity of parameters and data, not to check the integrity of firmware, Parameters and data are divided into multiple blocks based on different functional modules, with each block verifying a size of less than 512 bytes, this can ensures that the results obtained is same when calculation from the same data, and a different results obtained when calculation from different data.

status register is not set to 1, or the error bit is set to 1, or the output value is not random, such as all 0x00, all 0xFF, repeated values exceed a certain number.

7.3.5.2 Preservation of secure state

The TOE will do the following operations if related self-test fails.

1. There are some recovery mechanisms for the function parameters or data incomplete case. In case of the parameter incomplete, it will use backup data that read from external EEPROM, default data may be to use if the read data is incorrect also. In case of the important data incomplete, then will use backup data 1 read from external EEPROM, the backup data 2 may be to use if the backup data 1 is also incorrect. The backup mechanism can guarantee to one of the backup data is complete, because one of backup data saved only when the other one backup data is complete.
2. Record the corresponding event log and Push alarm to the system administrator or MCU reset if necessary. The Service Technician need to make some activity according to the event log and push alarm information.
3. Reconfigure the UART serial port and set the communication state machine to idle state waiting a communication request from external entity.
4. Use the clock which backup at every 15 minutes, then push a clock error to system administrator, after the system administrator received this error, normally it will cause a clock synchronization by system administrator.
5. If firmware validity check fails, reject start with this firmware and show error.
6. If a failure of random bit generator occurs during the power on initialization process, it initializes the random bit generator hardware. If a failure of random bit generator occurs during the communication process, it initializes the random bit generator hardware and rejects the current communication.
7. After resetting the meter, the MCU returns to its initial state, all hardware and software modules are initialized, parameters and data are rechecked to ensure validity, and then all functions are restarted and running normal.
8. Reset hardware/firmware/software applications that violate integrity and push an alarm to the system administrator if necessary.
9. System administrator will periodically get the TOE clock and compare it to system clock. If the deviation between TOE clock and system clock is too large, clock synchronization will be performed by system administrator.

7.3.6 Cryptographic operations

Since the meter is using Security Policy 3 every message is authenticated and encrypted.

Table 41 - Key description

Operation	Algorithm	Key size	Description
Encryption DLMS message encryption	AES-GCM-128	128 bits	Every message sent by the meter is encrypted with an AES-128 key based on the role used for communication.
Decryption DLMS message decryption	AES-GCM-128	128 bits	Messages sent to the meter with valid access rights are decrypted by the symmetric encryption keys corresponding to the used role.

Secure Hash DLMS generate message digest and Firmware Update generate image digest	SHA-256	-	Whether generate or verify digital signature values, it is necessary to first use the HASH algorithm to calculate the SHA256 digest value of the entire firmware package or DLMS messages, then use the signature algorithm with private/public key to generate/verify the signature value. Please see the Figure 15 Digital signatures process.
Digital Signature DLMS message signature and firmware update verification	ECDSA with P-256	Public Key:512bits Private Key:256 bits	Every firmware update and partial of DLMS message is digitally signed for verification. The meter verifies the digital signature of the new firmware and DLMS message before use. A private key will use for generating digital signature value when manufacturers want to release a new firmware. A public key will use for verifying digital signature value when TOE receives the new firmware. Please see the Figure 15 Digital signatures process.
Key wrap	AES-128 key wrap	128 bits	The key wrap function used to transfer one or more static or ephemeral symmetric keys. The key wrap algorithm is as specified by the DLMS security suite and AES key wrap algorithm is used in actual design of TOE to meet requirement. The key wrap algorithm using a 'key-wrapping key' (also known as a KEK: key encrypting key) to wrap keying material. The wrapped keying material can then be stored or transmitted securely. Unwrapping the keying material requires the use of the same 'key-wrapping key' that was used during the original wrapping process.
Key Agreement	ECDH with P-256	128 bits	Key agreement can be used to establish static keys between a server and a client or ephemeral keys between a server and a client or a third party. Different key agreement schemes are available to establish different keys. The Ephemeral Unified Model C(2e,0s, ECC CDH) scheme can be used by the client and the server to agreement out one or more static symmetric keys. To establish an ephemeral encryption key – used as the block cipher key – using key agreement, two schemes are

			available: One-Pass Diffie-Hellman C(1e, 1s, ECC CDH) scheme, Static Unified Model C(0e, 2s, ECC CDH) scheme. For the details of these Key agreement schemes please check the Annex C of [G-Book].

Figure 15 Digital signatures process

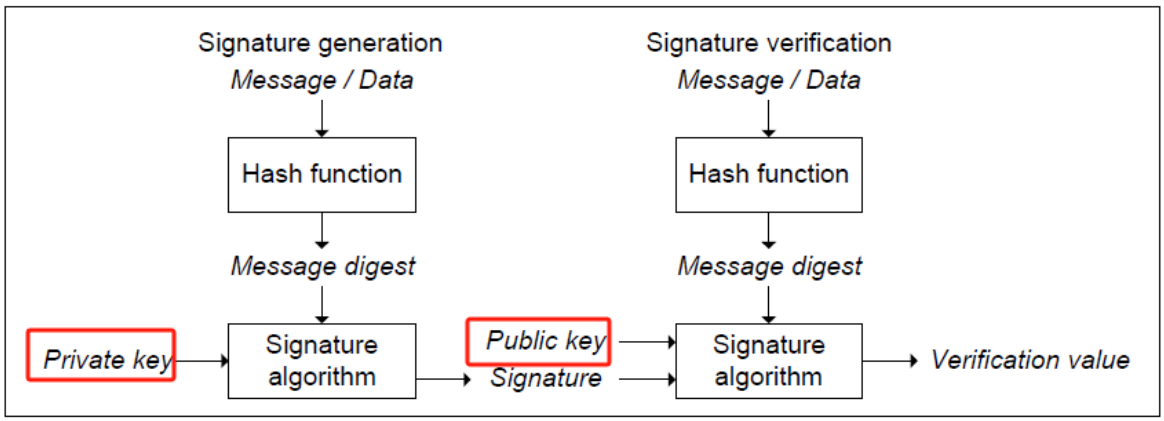


Figure 16 Ephemeral Unified Model C(2e, 0s, ECC CDH) scheme

C.1 Ephemeral Unified Model C(2e, 0s, ECC CDH) scheme

Figure C. 1 shows how the Ephemeral Unified Model C(2e, 0s, ECC CDH) scheme – specified in 9.2.3.4.6.2 – is used in DLMS/COSEM, by invoking the appropriate methods of the "Security setup" IC. See also 9.2.5.5.

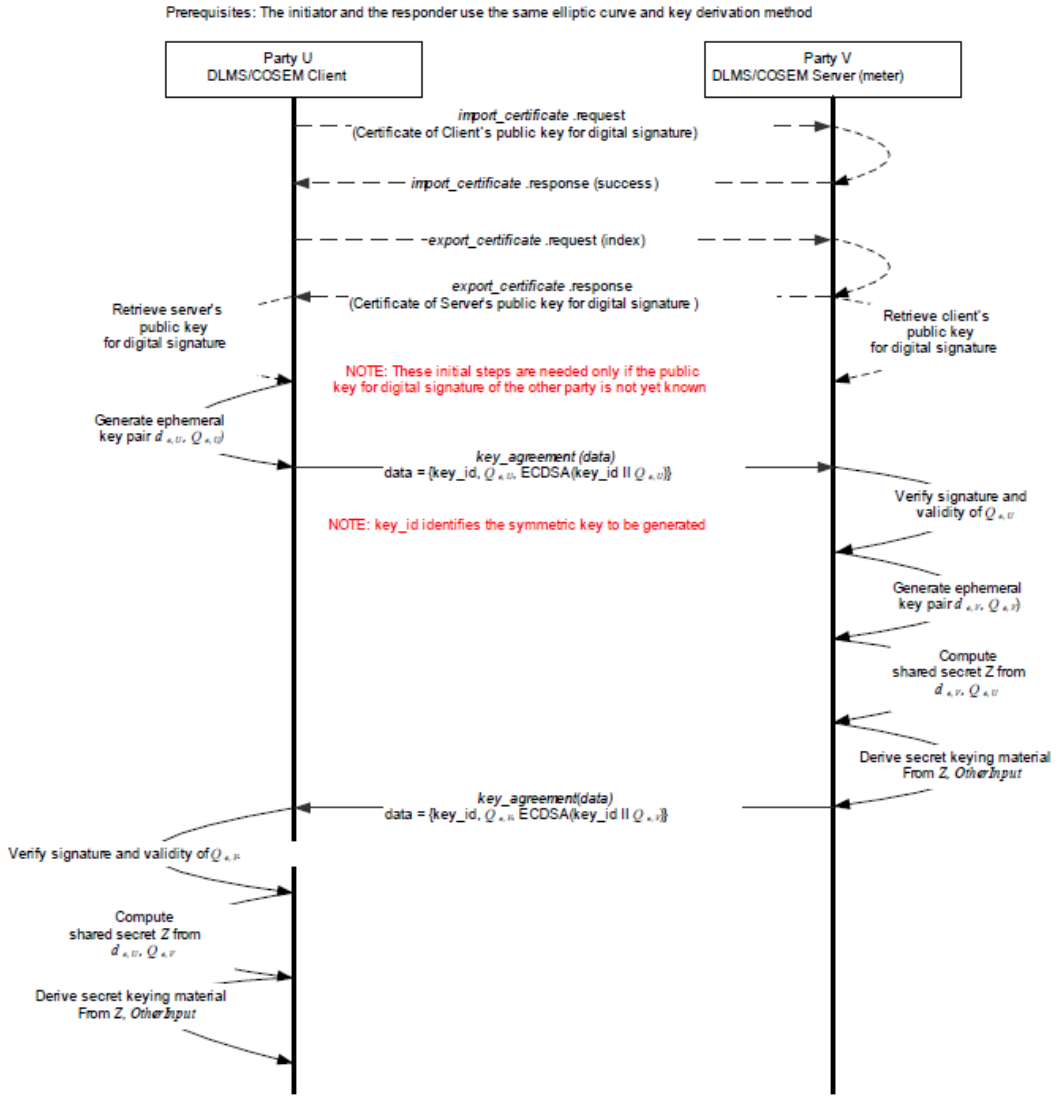


Figure C. 1 – MSC for key agreement using the Ephemeral Unified Model C(2e, 0s, ECC CDH) scheme

Figure 17 One-Pass Diffie-Hellman C(1e, 1s, ECC CDH) scheme

C.2 One-Pass Diffie-Hellman C(1e, 1s, ECC CDH) scheme

Figure C. 2 shows how the One-Pass Diffie-Hellman C(1e, 1s, ECC CDH) scheme, specified in 9.2.3.4.6.3 is used in DLMS/COSEM to protect an xDLMS APDU. See also 9.2.5.5.

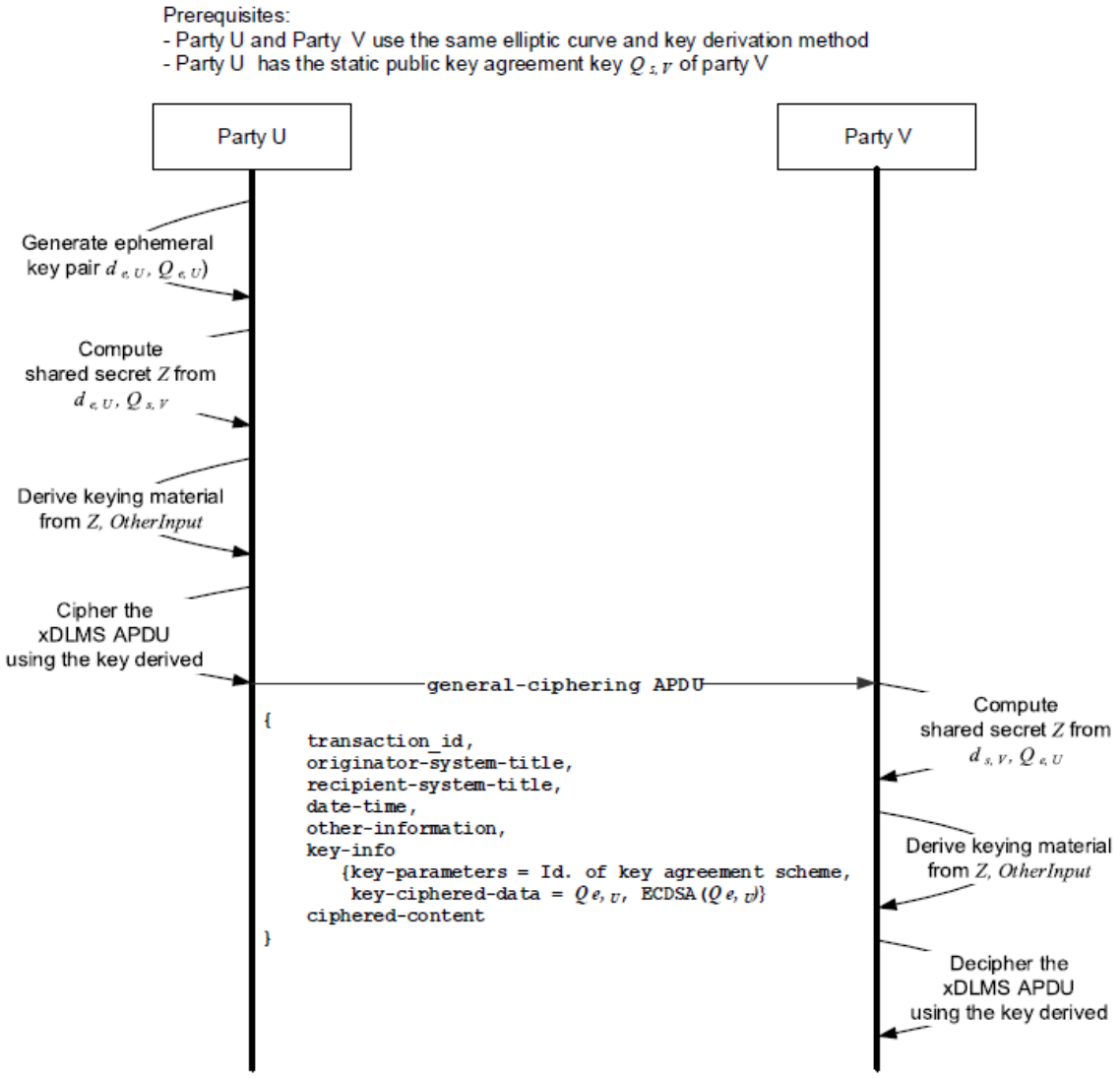


Figure C. 2 – Ciphered xDLMS APDU protected by an ephemeral key established using the One-pass Diffie-Hellman (1e, 1s, ECC CDH) scheme

Figure 18 Static Unified Model C(0e, 2s, ECC CDH) scheme

C.3 Static Unified Model C(0e, 2s, ECC CDH) scheme

Figure C. 3 shows how Static Unified Model C(0e, 2s, ECC CDH) schemes specified in 9.2.3.4.6.4 is used in DLMS/COSEM to protect an xDLMS APDU. See also 9.2.5.5.

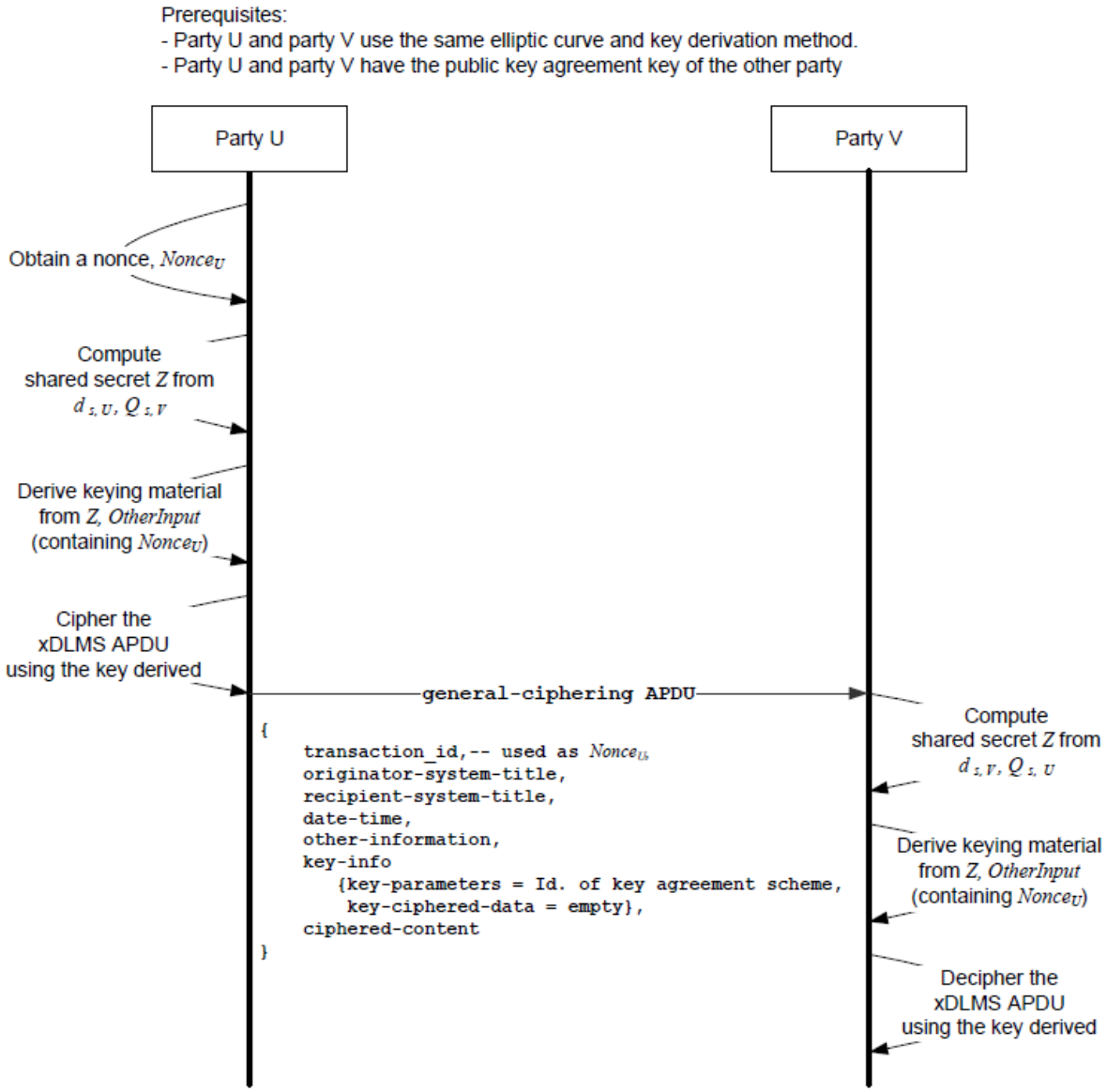


Figure C. 3 – Ciphered xDLMS APDU protected by an ephemeral key established using the Static Unified Model C(0e, 2s, ECC CDH) scheme

7.3.7 Random number generation

The random number generator is one peripheral of the MCU, it is using Fibonacci ring oscillator as entropy source, which can generate ns level random bit streams. Maximum support system frequency 29MHz output random number bit stream. Support address interleaving randomness enhancement algorithm. Support interrupt based output of 128 bit random numbers at a time.

There are many of algorithms used in DLMS/COSEM require generate the random numbers by random number generator (RNG), such as the following scenarios:

- Generate the challenge (random) when establish application layer links by HLS authentication mechanisms.
- Used for participating in message encryption.
- Used for generating ephemeral keys using key wrapping in each frame of communication.
- Used to generate private keys.

7.3.8 Key management

The key is the crucial parameter of the encryption algorithm. The management of the key is particularly important in TOE security protection, which mainly includes the following aspects.

7.3.8.1 Key generation

The keys in TOE can be divided into two types according to the encryption algorithm: symmetric type keys and asymmetric type keys. The different types of keys are generated by different key generation mechanisms.

The symmetric type keys are listed below, both client and TOE are using the same key.

- the master key, KEK; and/or
- the global unicast encryption key GUEK; and/or
- the global broadcast encryption key GBEK; and/or
- the (global) authentication key, GAK.
- Ephemeral encryption key.

The default values for these keys are provided in section 7.3.3. New keys can be generated by the client and then transmitted to TOE via the Key wrapping function. But there is no default value for the Ephemeral encryption key, it is generated by the key agreement function.

The asymmetric type keys are presented in pair that listed below, there are private key and public key in each pair.

- Digital signature key pair
- Static key pair
- Ephemeral key pair

About the key generation algorithm from [G-Book]: An ECC key pair d and Q is generated for a set of domain parameters (q, FR, a, b {, domain_parameter_seed}, G, n, h). Two methods are provided for the generation of the ECC private key d and public key Q; one of these two methods shall be used to generate d and Q. Prior to generating ECDSA key pairs, assurance of the validity of the domain parameters (q, FR, a, b {, domain_parameter_seed}, G, n, h) shall have been obtained. For details, see [FIPS PUB 186-5], Annex B.4.

The digital signature key pair is produced by the manufacturer using the key generation algorithm, the private key is kept confidential by the manufacturer, and the public key is delivered or updated to the TOE in the form of a certificate by use import certificate method of class id 64.

Both the client and TOE have their own static key pairs. For the client static key pair, the client manages the static key pair and delivered or updates the public key to TOE in the form of a certificate. For the TOE static key pair, the client sends a request to the TOE to generate a static key pair. The TOE keeps the private key confidential, sends the public key to the client to apply for a public key certificate, then import to TOE to verify certificate, finally, exports the public key certificate to obtain the official public key of the TOE.

In general, the Ephemeral key pair is generated for key agreement function, it is generated a pair each client and server when use Ephemeral Unified Model C(2e,0s, ECC CDH) scheme, either, it is generated by client when use One-Pass Diffie-Hellman C(1e, 1s, ECC CDH) scheme. For details about the schemes see section 7.3.6.

7.3.8.2 Key destruction

The symmetric key types. Static keys that are intended to be used for a relatively long period of time. In DLMS/COSEM these may be:

- A global key that may be used over several AAs established repeatedly between the same partners. It will keep until make an operation of update new keys.
- A dedicated key that may be used repeatedly during a single AA established between two partners. Therefore, its lifetime is the same as the lifetime of the AA, and it will clear to zero destruction by end of the AA.

Ephemeral keys used generally for a single exchange within an AA. It will clear to zero destruction by end of the AA.

The asymmetric key types. The client public key certificate (when no longer needed) can be destroyed by use remove certificate method of class id 64 [B-Book].

Figure 19 - Remove certificate from the server

9.2.6.6.7 Certificate removal from the server

It is sometimes necessary to remove a public key certificate stored by the server.

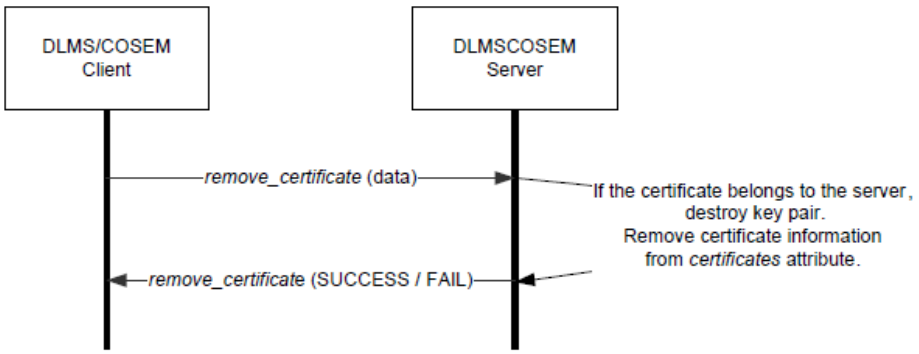
NOTE 1 This may relate to certificates that belong to the server or certificates that belong to a client or third party.

NOTE 2 The conditions when removal of a public key certificate is necessary are out of the Scope of this Technical Report.

When a certificate that belongs to the server is removed, the private key associated with the public key shall be destroyed.

The information on the certificate removed shall be also removed from the *certificates* attribute of the "Security setup" object.

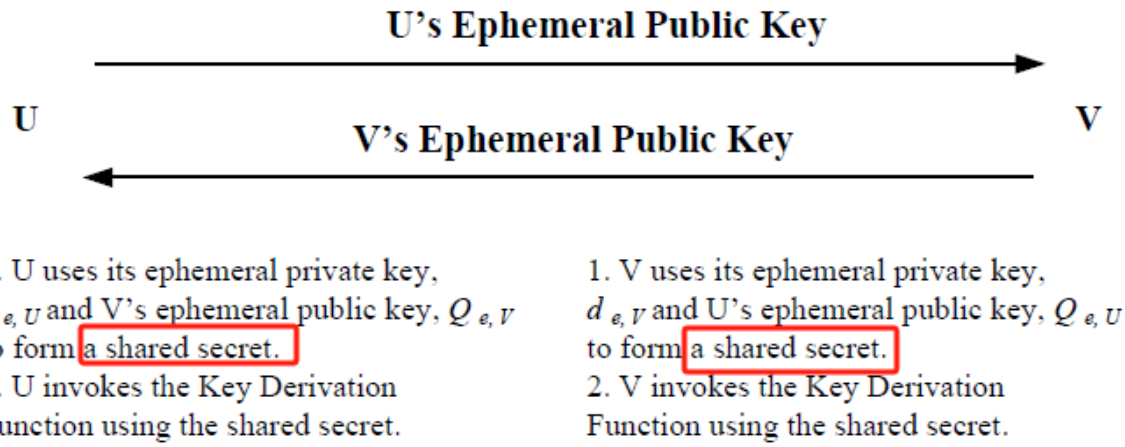
The key pair the public key certificate of which has been removed cannot be used any more for transactions. The process is shown in Figure 105.



NOTE The *remove_certificate* (data) method may be also invoked by a third party, using the client as a broker.

In the process of key agreement when use the Ephemeral Unified Model C(2e,0s, ECC CDH) scheme, the shared secret Z value is generated, which is use for deriving secret keying material, so it will be destroyed immediately by clear to zero after use.

Figure 20 - Key agreement



7.3.8.3 Key management

For the symmetric key type, the key management mainly includes the key transfer and update, the key agreement, the key protection, the key destruction and so on. During the interaction between the client and TOE, all keys are highly confidential and require corresponding permissions to be updated.

For the asymmetric key type, the key management includes the process of generating public and private key pairs, applying for generating public key certificates, importing and exporting certificates, and removing certificates. During the interaction between the client and TOE, there is no transmission of private keys to prevent leakage.

There is no read access permission provided to plaintext private or secret keys stored in the TOE. All values of the key itself or values related to key agreement will be immediately clear to zero and destroyed when no longer needed.

A key with incorrect type or length is always rejected by the TOE.

All information related to key management in TOE is explained in the above. For more details, please see [G-Book] section 9.2 Information security in DLMS/COSEM.

7.3.9 Access control

The 'metrologically certified data' is the encrypted meter data stored in the external EEPROM, 'credentials' are the keys used throughout the communication because the meter is using the DLMS/COSEM authentication processes with symmetric keys instead of username and password, or any other authentication method, 'meter configuration' is the meters configuration data and parameterization, which can be modified by specific roles with specific authorizations, and record data (Load profile, end of billing, event log) is the stored records in the meter.

Metrologically certified data include total energy and rate energy can only be read by Reader, Administrator and Operator.

Credentials include:

- Master Key, Global Unicast Encryption Key (GUEK), Global broadcast key(GBEK), Authentication key(AK) for each user roles, cannot be read and only be update by Administrator with key wrapper.
- LLS password for each user roles, cannot be read and only be update.
- Policy only be update by Administrator, read by the Reader, Administrator and Operator.
- Meter configuration: Alarm Filters decision which alarm occur will push alarms, only can update by Administrator and Operator.

Firmware cannot be accessed because the firmware of the meter is stored in the Flash memory inside the MCU. No interface provided for external access. The firmware upgrade operation is the only way to modify it, but this must via a secure update process (the relevant update process is details in FPT_TSU.1, see section 6.3.4.6). In brief, the prerequisite is the user role own the corresponding permissions and got a correct image with a digital signature release from manufacture.

7.4 Push

In most cases the messages are sent to the system administrator, which means the responsible personal from the electricity service provider.

7.4.1 Meter Registration

7.4.1.1 General

The registration operation is the meter announcement at the management level when the meter is installed on the field for the first time. For the wireless WAN devices, the registration is performed with the means of push operation by pressing button 5 seconds. This registration is required after the TOE is in its secure operational state, and this registration is related to the electricity service provider's network.

7.4.1.2 Objects

The following objects are mandatory for the registration use case

Push setup – On installation	Class Id 40	Logical name 0-7:25.9.0.255
Logical device name	Class Id 1	Logical name 0-0:42.0.0.255
Device ID 1 (manufacturing number)	Class Id 1	Logical name 0-0:96.1.0.255

The device ID 1 holds the meter unique identification number, defined according to the Utility requirements. The meter unique identification number should be displayed as barcode on the meter's nameplate.

7.4.2 Push Setup – Interval_1

For wireless WAN devices, the End of Billing data may be collected using pull mode, by sending the appropriate request to the server.

In addition with the pull mode, the End of Billing data may be collected using Push mode.

The following objects are required for the management of the End of Billing Period Push:

Push setup - interval 1	Class Id 40	Logical name 0-1:25.9.0.255
Push action scheduler - interval 1	Class Id 22	Logical name 0-1:15.0.4.255
Push script table	Class Id 9	Logical name 0-0:10.0.108.255
Data of end billing period 1	Class Id 7	Logical name 0-0:98.1.0.255

7.4.3 Push Setup – Interval_2

All the logbooks may be read by request / response using pull mode, by the management client for wireless WAN meters. Additionally, for wireless WAN meters data collection, the logbooks data collection on a daily or weekly basis is possible using push mode, with or without selective access. Several logbooks may be retrieved using the same push setup object. Push setup interval 2 shall be used for this purpose.

The following instances allow the management of the logbooks data collection using Push:

Push set up – interval 2	Class Id 40	Logical name: 0-2:25.9.0.255
Push action scheduler – interval 2	Class Id 22	Logical name: 0-2:15.0.4.255
Push script table	Class Id 9	Logical name: 0-0:10.0.108.255
Standard logbook	Class Id 7	Logical name: 0-0:99.98.0.255
Fraud logbook	Class Id 7	Logical name: 0-0:99.98.1.255
Communication logbook	Class Id 7	Logical name: 0-0:99.98.5.255

7.4.4 Push Setup – Interval_3

For wireless WAN devices, the active energy import(+A) data may be collected using pull mode, by sending the appropriate request to the server.

In addition, with the pull mode, the active energy import(+A) data may be collected using Push mode.

The following objects are required for the management of the active energy import(+A) Period Push:

Push setup - interval 3	Class Id 40	Logical name 0-3:25.9.0.255
Push action scheduler - interval 3	Class Id 22	Logical name 0-3:15.0.4.255
Push script table	Class Id 9	Logical name 0-0:10.0.108.255
Active energy import(+A)	Class Id 3	Logical name 1-0:1.8.0.255

7.4.5 Push Setup – On Alarm

7.4.5.1 Process

Some of the events can trigger alarms. If one of these events occurs, the corresponding flag in the alarm registers are set and an alarm is then raised via communication channel. All alarm flags in the alarm registers remain active until the alarm registers are cleared. Each bit in the alarm registers represents a different alarm. If the bit is set (logical 1) the alarm (corresponding to position of the set bit) was recorded.

The value in the Alarm Registers is a summary of all active and inactive alarms at that time. Depending on the capabilities of the system and the policy of the utility, not all possible alarms are wanted. Therefore, the Alarm Filters can be programmed to mask out unwanted alarms.

The structure of the filter is the same as the structure of the Alarm Registers. To mask out unwanted alarms the corresponding bits in Alarm Filters should be set to logical 0.

Alarm Registers (AR)

All information on the “cause of the alarm” of the meter is contained in the Alarm Registers.

Specific bits of Alarm Registers may be internally reset if the “cause of the alarm” has disappeared (e.g. bit1 (battery replace) if the battery has been exchanged). Alternatively, all bits may be externally reset by the client by executing a SET =0 service to the Alarm Registers attribute value (e.g. bit 13 (Fraud attempt) can only be externally reset). In the latter case those bits for which the “cause of alarm” still exists will be set to 1 again and an alarm will be issued.

Alarm Descriptors (AD)

The Alarm Descriptors have the same structure as the Alarm Registers. Whenever a bit in the Alarm Registers changes from 0 to 1, then the corresponding bit of the Alarm Descriptors (AD) is set to 1. Resetting the Alarm Registers does not affect the Alarm Descriptors. The set bits of the AD must be reset explicitly by the system administrator.

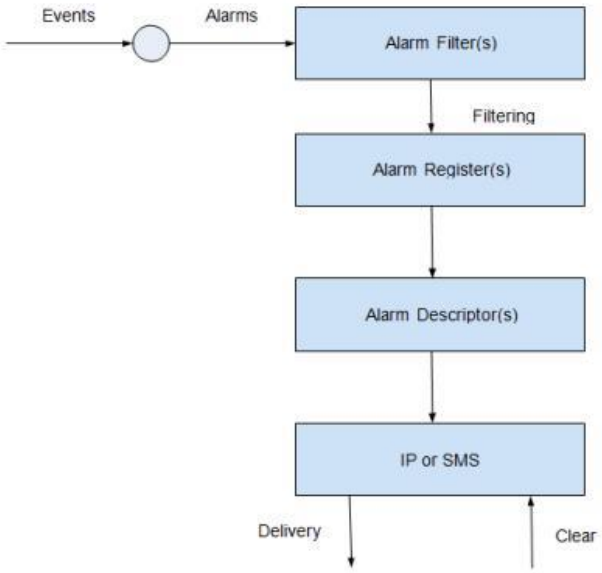
Alarming Process

The Alarm Descriptors are sent to the system administrator using the Data-Notification service triggered by the corresponding Alarm Monitor. In IDIS package 2 the Alarm Monitor Threshold value is set to zero. Therefore, the Alarm Monitor action is invoked when any of the bits in the Alarm Descriptors value changes from 0 to 1.

To acknowledge the reception of the Alarm the system administrator must reset the Alarm Descriptors by invoking the SET=”with bits set to 1 which need to be cleared” on the Alarm Descriptors value. Upon reception of this SET service, the meter clears the corresponding bits in the Alarm Descriptors.

To re-enable the alarm reporting process, the system administrator must reset the reported bits in the Alarm Register. This can only be done by setting all the bits of the Alarm Registers to 0 using the SET service. Prior to this action the system administrator must read the latest value of the Alarm Register.

Figure 21 - push alarm process



7.4.5.2 Objects

The following objects related must be supported:

Error Register	Class Id 1	Logical name: 0-0:97.97.0.255
Error Register 2	Class Id 1	Logical name: 0-0:97.97.1.255
Alarm Register 1	Class Id 1	Logical name: 0-0:97.98.0.255
Alarm Register 2	Class Id 1	Logical name: 0-0:97.98.1.255
Alarm Filter 1	Class Id 1	Logical name: 0-0:97.98.10.255
Alarm Filter 2	Class Id 1	Logical name: 0-0:97.98.11.255
Alarm Descriptor 1	Class Id 1	Logical name: 0-0:97.98.20.255
Alarm Descriptor 2	Class Id 1	Logical name: 0-0:97.98.21.255
Alarm Monitor 1	Class Id 21	Logical name: 0-0:16.1.0.255
Alarm Monitor 2	Class Id 21	Logical name: 0-0:16.1.1.255
Push script table	Class Id 9	Logical name 0-0:10.0.108.255
Push setup – On alarm	Class Id 40	Logical name: 0-4:25.9.0.255

7.4.5.3 Alarm Register 1 and Error Register Bits

Reference IDIS pack 2.0 7.3.2.3

Table 42 - Alarm Register 1

Bit	Alarm	Triggering event
0	Clock invalid	6
1	Battery replace	7

2	Reserved for future use	-
3	Reserved for future use	-
4	Reserved for future use	-
5	Reserved for future use	-
6	Reserved for future use	-
7	Reserved for future use	-
8	Program memory error	12
9	RAM error	13
10	NV memory error	14
11	Measurement system error	16
12	Watchdog error	15
13	Fraud attempt	40, 42, 44, 46,49, 50
14	Reserved for future use	-
15	Reserved for future use	-
16	Reserved for future use	100
17	M-Bus communication error ch1	110
18	M-Bus communication error ch2	120
19	M-Bus communication error ch3	130
20	M-Bus communication error ch4	103
21	M-Bus fraud attempt ch1	113
22	M-Bus fraud attempt ch2	123
23	M-Bus fraud attempt ch3	133
24	M-Bus fraud attempt ch4	106
25	Permanent error M-bus ch1	116
26	Permanent error M-bus ch2	126
27	Permanent error M-bus ch3	136
28	Permanent error M-bus ch4	102
29	Battery low on M-bus ch1	112
30	Battery low on M-bus ch2	122
31	Battery low on M-bus ch3	13

7.4.5.4 Alarm Register 2 Bits

Reference IDIS pack 2.0 7.3.2.4

Table 43 - Alarm Register 2

Bit	Alarm	Triggering event
0	Total Power Failure	01
1	Power Resume	02
2	Voltage Missing Phase L1	82
3	Voltage Missing Phase L2	83
4	Voltage Missing Phase L3	84
5	Voltage Normal Phase L1	85
6	Voltage Normal Phase L2	86
7	Voltage Normal Phase L3	87
8	Missing Neutral	89
9	Phase Asymmetry	90
10	Current Reversal	91
11	Wrong Phase Sequence	88
12	Unexpected Consumption	52
13	Key Exchanged	48
14	Bad Voltage Quality L1	92

15	Bad Voltage Quality L2	93
16	Bad Voltage Quality L3	94
17	External Alert	20
18	Local communication attempt	158
19	New M-Bus Device Installed Ch1	105
20	New M-Bus Device Installed Ch2	115
21	New M-Bus Device Installed Ch3	125
22	New M-Bus Device Installed Ch4	135
23	Reserved for future use	-
24	Reserved for future use	-
25	Reserved for future use	-
26	Reserved for future use	-
27	M-Bus valve alarm Ch1	164
28	M-Bus valve alarm Ch2	174
29	M-Bus valve alarm Ch3	184
30	M-Bus valve alarm Ch4	194
31	Disconnect/Reconnect Failure	68

7.4.6 Push Setup – On Connectivity

The network connectivity of an IDIS meter is controlled by the auto connect objects and the Push setup – On Connectivity. When meter module is on-line, and push object & address is right, then meter will auto push data to the system administrator.

Auto connect	Class Id 29	Logical name: 0-0:2.2.1.255
Push setup – On connectivity	Class Id 40	Logical name: 0-0:25.9.0.255

7.5 Firmware Upgrade

7.5.1 Overview

The meter supports local update via local communication port (IR or RS485) or remote ports (GPRS) and adopts DLMS to upgrade meter’s firmware.

The meter will auto execute the new program after updating. During the process of remote update, the meter must keep power-on.

The firmware update for the meter and its communication module should be executed remotely via the system administrator or the manufacturer's system, as per data protection regulations.

This process involves encrypted and key-protected updates and remote parameterization, ensuring the authentication and DSO seal remain intact.

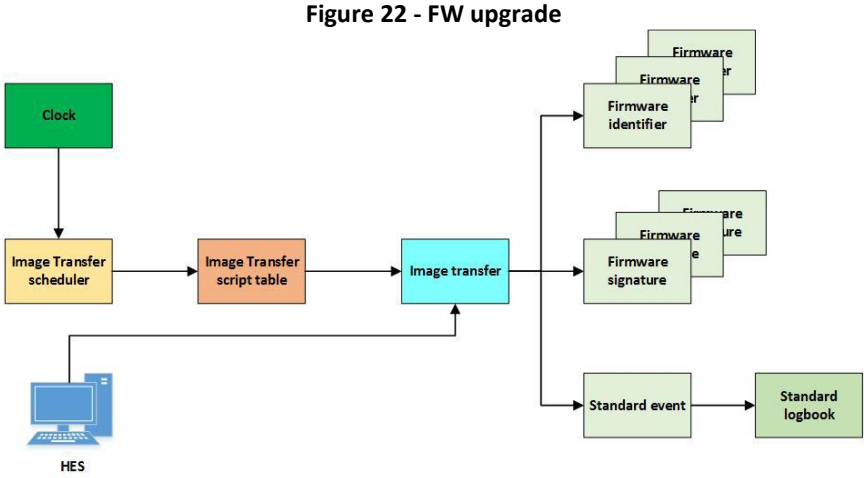
The firmware update must only be possible after the authenticity of the firmware update has been verified and if the version number of the new firmware is higher to the version of the installed firmware. It's crucial that the firmware update does not affect the stored data, change the device's measuring capabilities, or render the existing driver unsuitable for remote reading operations.

Administrator and Supervisor (Operator) are allowed to upgrade the firmware with separate keys.

7.5.2 Process

The firmware upgrade shall be as according to DLMS. The process of the firmware upgrade is as shown:

Figure 22 - FW upgrade



As the definition of Class_id 18 in the [B-Book], the firmware upgrade process usually includes the following 4 steps:

1. The client initiates the Image transfer process in servers by invoking the image_transfer_initiate method. After a successful initiation, all the image upgrade process status will go back to the initial value.
2. The client transfers image blocks one by one to server by invoking the image_block_transfer method, the TOE received the image blocks then stored in the internal data flash, the image file contains the firmware itself and its digital signature.
3. Verifies the integrity of the Image by the TOE after all blocks have transfers over and before activation. This can be initiated by invoking the image_verify method by the client or it may be initiated also by the TOE.

   The verification process is to determine the version information and digital signature to determine the integrity and authenticity of the image.

   The version information includes hardware version and firmware version, Only when the hardware version information of the new firmware matches the actual hardware and the software version is larger than the current one can it pass the version information verification.

   The digital signature verification is use ECDSA with P-256, the main process is using the HASH algorithm to calculate the SHA256 digest value of the entire firmware package, then use the public key used for firmware upgrade to verify this SHA256 digest value and the digital signature value carried by the Image package, if the verify operation return a success can pass the digital signature verification. This can ensure that the firmware image using in the upgrade operational is released by the manufacture, and it is not counterfeited or tampered in the image transmission process.

4. Activates the Image by TOE. This can be initiated by invoking the image_activate method by the client or it may be initiated also by the TOE. If the activation is done

without a previous verification, then verification is done implicitly as part of the activation.

The activate process carried out in two steps, first, copy the currently running firmware to the data flash as a backup, then jump to the Bootload and activate the new firmware to app code area and execute it. If the new firmware starts up failure many times, the fall-back mechanism will worked that use the previous(backup) firmware ensure the TOE have a correctly firmware to run.

The following instances allow the management of the firmware upgrade.

Image transfer	Class Id 18	Logical name 0-0:44:0.0.255
Active firmware identifier	Class Id 1	Logical name 1-0:0.2.0.255
Active firmware signature	Class Id 1	Logical name 1-0:0.2.8.255
Image activation script table	Class Id 9	Logical name 0-0:10.0.107.255
Image activation single action scheduler	Class Id 22	Logical name 0-0:15.0.2.255
Standard logbook event	Class Id 1	Logical name 0-0:96.11.0.255
Standard logbook	Class Id 7	Logical name 0-0:99.98.0.255

Note: The events related to the image transfer management are handled by the standard logbook event and standard logbook.

7.6 Meter Communication

Any interface other than those in FDP_IFF.1.2/Int is disabled.

7.6.1 Interface 1 – Optical port

Meter has an optical port, which can support direct HDLC or Mode E(IEC 62056-21).

If direct HDLC, the following objects should be supported:

IEC HDLC port setup	Class Id 23	Logical name 0-0:22:0.0.255

If Mode E, the following objects should be supported:

Optical port setup	Class Id 19	Logical name 0-0:20:0.0.255

For details see [UM] section 4.14.2 Interface 1 (Optical port)

7.6.2 Interface 2 – RS485

Meter have a RS485 port, which can support direct HDLC, the following objects should be supported:

IEC HDLC port setup	Class Id 23	Logical name 0-0:22:0.0.255

For details see [UM] section 4.14.3 Interface 2 (RS485).

7.6.3 Interface 3 – Communication module

Meter has a port for CAT1/CAT M1 module, between meter and module TTL communication speed is 9600bps, the system and meter communication use DLMS protocol for transparent transmission. The following objects should be supported for CAT1/CATM1 module:

Auto connect	Class Id 29	Logical name 0-0:2:1.0.255
Auto answer	Class Id 28	Logical name 0-0:2:2.0.255
TCP-UDP setup	Class Id 41	Logical name 0-0:25:0.0.255
IPV4 setup	Class Id 42	Logical name 0-0:25:1.0.255

IPV6 setup	Class Id 48	Logical name 0-0:25:7.0.255
GPRS modem setup	Class Id 45	Logical name 0-0:25:4.0.255
PPP setup	Class Id 44	Logical name 0-0:25:3.0.255
Modem configuration	Class Id 27	Logical name 0-0:2:0.0.255

For details see [UM] section 4.14.3 Interface 3 (Module port).

7.6.4 Interface 4 – P1 port

Meter have a P1 port.

Physical connector pin assignment of passive mode according to DSMR5.0.2.

For details see [UM] section 4.14.5 Interface 4 (P1 port).

7.7 Security Functional Requirements rational

Table 44 - SFR coverage

7.1 Real-Time Clock 7.2 Event Log 7.3 Security 7.4 Push 7.5 Firmware Upgrade 7.6 Meter Communication	**7.1**	**7.2**	**7.3**	**7.4**	**7.5**	**7.6**
FCS_CKM.1			X			
FCS_CKM.4			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			X
FDP_IFF.1/Int			X			X
FDP_IFC.1/Keys			X	X	X	X
FDP_IFF.1/Keys			X	X	X	X
FDP_RIP.1			X			
FIA_UAU.6			X			X
FIA_AFL.1			X			X
FPT_BST.1			X			
FPT_FLS.1		X	X			
FPT_TNN.1		X	X	X		X
FPT_RPL.1			X			X
FPT_STM.1	X					
FPT_TSU.1					X	X
FMT_SMR.1			X			
FMT_MOF.1			X	X	X	X
FMT_MTD.1/Audit		X	X			
FMT_MTD.1/Time			X			
FAU_ARP.2		X				X
FAU_GEN.1		X	X			
FAU_SAR.1		X	X			X
FAU_SAR.2			X			X

7.1 Real-Time Clock 7.2 Event Log 7.3 Security 7.4 Push 7.5 Firmware Upgrade 7.6 Meter Communication	7.1	7.2	7.3	7.4	7.5	7.6
FAU_STG.1		X	X			
FAU_STG.3		X	X			

8 Glossary

Table 45 – Glossary

Term	Meaning
AA	Application Association
Administrator	Entity that has a level of trust with respect to all policies implemented by the TSF – see [CC_P1]. The Administrator role is referred to in SFRs in section 6.3 as a generic term for a privileged role that has access to sensitive operations affecting the configuration and operation of the meter.
AES	Advanced Encryption Standard
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 [CC_P1].
CC	Common Criteria
COSEM	Companion Specification for Energy Metering
Consumer	End user of the metered quantity
Critical Event	An event that can take place in a smart meter and that is particularly significant for supply or security of the meter.
CRC	Cyclic Redundancy Check
DLMS	Device Language Message Specification
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).
ECDH with P-256	Elliptic Curve Diffie-Hellman key agreement protocol with curve P-256
ECDSA	Elliptic Curve Digital Signature Algorithm specified in ANSI X9.62 and FIPS PUB 186-5:2019
Evaluator	The person or group that carries out a security evaluation of the TOE, using the criteria in [CC_P1],

	[CC_P2] and [CC_P3] and the associated methodology in [CC_P4].
External Entity	See 'User'.
FW 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).
GCM	Galois/Counter Mode, an algorithm for authenticated encryption with associated data
HDLC	High level Data Link Control
HES	Head End System
HLS5	High Level Security HLS-5 (using AES-GMAC)
IT	Information Technology
IDIS2.0	Interoperable Device Interface Specifications V2.0
Local Network	Data communication network providing access to local (in house/building) devices and/or other local networks
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).
MDM	Metering Data Management
Meter data	Meter readings that allow calculation of the quantity of electricity 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)
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)
Neighbourhood Network	Data communication network providing access to several premises and/or other neighbourhood networks
OSP	Organizational Security Policy
Operational Interfaces	Interfaces required for normal operation of the meter (all other accessible interfaces are disabled)
PP	Protection Profile
Role	The entitlement of a party to execute a set of one or more commands associated with the role name.
SA	Security Association

SAR	Security Assurance Requirement
SAP	Service Access Point
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.
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
ST	Security Target
TOE	Target of Evaluation
TOU	Time of use
TSF	TOE Security Functionality
TSF Data	Data for the operation of the TSF upon which the enforcement of the requirements relies – see [CC_P1].
User	Human or IT entity interacting with the TOE from outside of the TOE boundary (based on [CC_P1]).
WAN Wide Area Network	extended data communication network connecting a large number of communication devices over a large geographical area

9 Bibliography

[CC_P1] Common Criteria, Part 1: Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001

[CC_P2] Common Criteria, Part 2: Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002

[CC_P3] Common Criteria, Part 3: Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003

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

[SM_MSR] Protection Profile for Smart Meter Minimum Security requirements, Version: 1.0, Date: 2019-10-30, Authors: Ad-Hoc Group Privacy & Security of the CEN/CENELEC/ETSI Coordination Group on Smart Meters

[B-Book] Blue Book Edition 15 - COSEM Interface Classes and OBIS Object Identification System DLMS UA 1000-1 Ed. 15, 2021-12-23

[G-Book] Green Book Edition 11 - DLMS/COSEM Architecture and Protocols DLMS UA 1000-2 Ed.11, 2021-12-21

[IDIS-ID] IDIS INTEROPERABILITY SPECIFICATION Package 2 IP Profile Edition 2.0 (including G3-PLC), 03-09-2014

[IDIS-SM] IDIS Interoperability specification – Package 2 – Smart Metering Objects Edition 2.0 (including G3-PLC), 03-09-2014

[UM] Wasion aMeterx00 Smart Energy Meter User Manual, version: v1.0, date: 2024-03-25 (aMeterx00 Smart Energy Meter User Manual_20240325.pdf)

[EQ-Report] Equivalency Report for WASION aMeter100 and aMeter300 Smart Energy Meters, version: v1.2, date: 2025-03-11

[AGD] AGD Documentation WASION aMeter100 and aMeter300 Smart Energy Meters, v1.5, 2025-05-19

[RFC 3394] Schaad, J. and R. Housley, "Advanced Encryption Standard (AES) Key Wrap Algorithm", RFC 3394, DOI 10.17487/RFC3394, September 2002, https://www.rfc-editor.org/info/rfc3394

[NIST SP 800-56A] NIST SP 800-56A Rev. 3 Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography Date Published: April 2018

[IEC62056-53] Electricity metering data exchange – The DLMS/COSEM suite – Part 5-3: DLMS/COSEM application layer

[IEC62056-62] Electricity Metering Data Exchange – The DLMS/COSEM suite – Part 6-2: COSEM interface classes.

[FIPS 140-2] FIPS 140-2 Security Requirements for Cryptographic Modules Date Published: May 25, 2001 (Change Notice 2, 12/3/2002)

[NIST SP 800-38D] NIST SP 800-38D Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC Date Published: November 2007

[FIPS PUB 186-5] FIPS 186-5 Digital Signature Standard (DSS) Date Published: October 2019

[FIPS PUB 180-4] FIPS 180-4 Secure Hash Standard (SHS) Date Published: August 2015

[DLMS_OLIST] Hungary Object list v1.2 20250507.xlsx

[DIN 43863-3] DIN 43863-3:1997, Electricity meters – Part 3: Tariff metering device as additional equipment for electricity meters – EDIS – Energy Data Identification System, 1997-02, https://www.beuth.de/de/norm-entwurf/din-43863-3/2903391