SANXING

Security Target

SANXING SX601 and SX631 Smart Meters
Evaluation Assurance Level (EAL): EAL3 augmented with ALC_FLR.3.

TOE Full Name:	SANXING SX601 1 phase and SX631 3 phase Smart Meter
Version	V2.0
Date	2025-11-04
Classification:	PUBLIC

Version history

Version	Date	Author	Description
v1.0	2024-02-28	SANXING ODD	The first version of the Security Target.
v1.1	2024-05-15	SANXING ODD	Amendments based on the 1st analysis cycle.
v1.2	2024-07-08	SANXING ODD	Amendments based on the 2nd analysis cycle.
v1.3	2024-07-25	SANXING ODD	Amendments based on the ADV document.
v1.4	2024-11-18	SANXING ODD	Amendments based on the 3rd analysis cycle.
v1.5	2025-02-27	SANXING ODD	Amendments based on the 2nd analysis cycle of ADV, AGD, ALC.
v1.6	2025-05-28	SANXING ODD	Amendments based on the 4th analysis cycle
v1.7	2025-06-20	SANXING ODD	Amendments based on the 5th analysis cycle
v1.8	2025-09-23	SANXING ODD	Amendments based on the SXEV601631-052_OCSI_findnings_v1
v1.9	2025-10-28	SANXING ODD	Amendments based on the email on 2025/10/27
V2.0	2025-11-04	SANXING ODD	Amendments based on the email on 2025/11/03

Table of Contents

1 Introduction

1.1 ST Reference

Table 1 - ST Reference

ST Title	SANXING SX601 and SX631 Smart Meters
ST Version	V2.0
ST Creation Date	2025-11-04

1.2 TOE Reference

Table 2 - TOE Reference

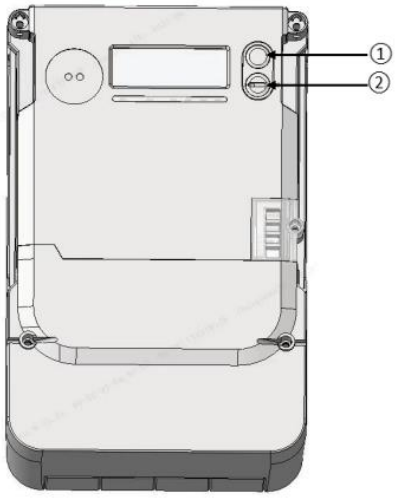
TOE Full Name	SANXING SX601 1 phase and SX631 3 phase Smart Meter
TOE Version	SX601 • Hardware version: S12U26 S15.Y4.J0 M12 • Metrological FW version: V0.03.10 • Application FW version: E.S12U26.HU.007179.V1.00.33 SX631 • Hardware version: S34U28 S38.Y2.J0 M11 • Metrological FW version: V0.10.10 • Application FW version: E.S34U28.HU.007178.V1.00.33
TOE Short Name	SANXING Smart Meter

Note: The TOE short name is used through this document to refer to the TOE.

1.3 TOE Overview

SX601 and SX631 family is designed for measuring and monitoring energy parameters. The name of the 1phase Smart Meter is SX601, and the 3phase is SX631. The TOE can be programmed and configured locally through 2 interfaces, which are the optical interface (P0) and the RS-485 interface. The TOE also has remote access. through cellular network. It supports the following standards: GPRS/4G, LTE-M. There are an LCD display and 2 push-buttons. The 2 buttons perform two different functions, the first button's function is to scroll the information on the LCD display, the second button's function is to reconnect the circuit breaker. The second button is sealable, so its pressing can be traced. The meter does not measure its own consumption.

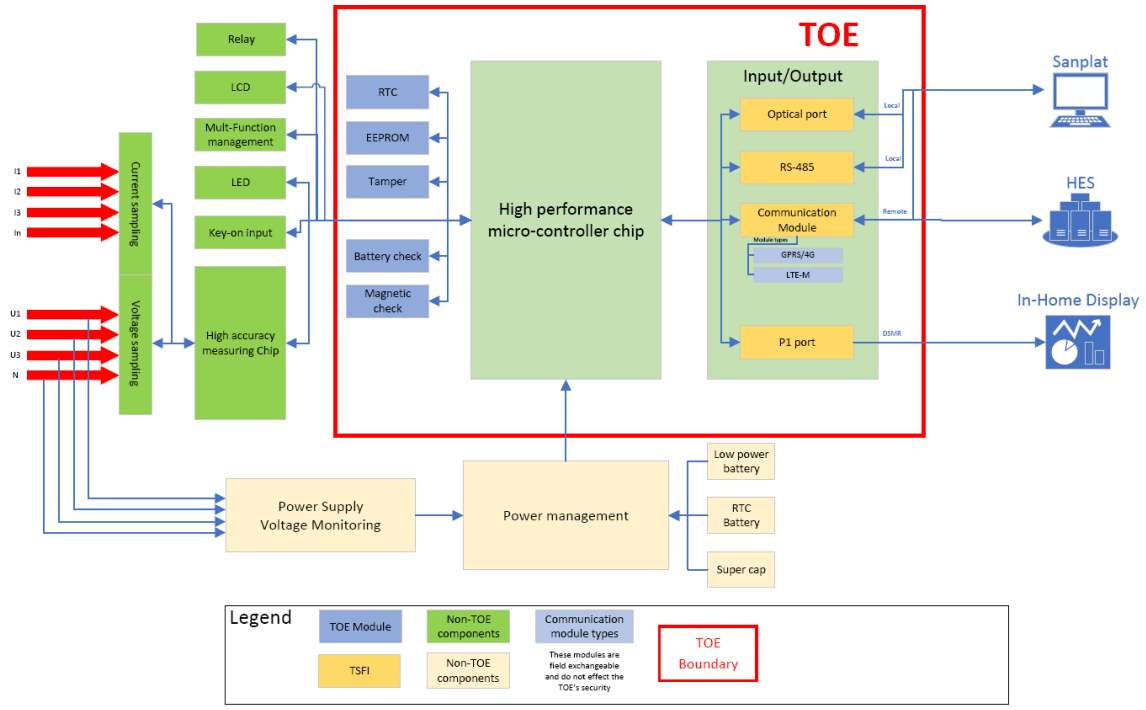
Figure 1- TOE Push buttons



The types of electricity are divided into basic electricity and combined electricity. Each type of electricity is generally stored in the meter in two ways, the first is the cumulative electricity form, and the second is the interval electricity form. Most electricity is allocated to RAM storage space and external non-volatile storage space, and some electricity is obtained by electricity combination calculation when reading.

1.3.1 TOE Boundary

Figure 2 - TOE boundary



There are 2 types of devices, the main difference between them is the metrological part of the meters. SX601 is a 1-phase and SX631 is a 3-phase smart meter. The two devices are otherwise almost equal. The manufacturer provided an equivalency report [EQ-Report] to detail the subtle differences and the equivalency of the functionalities of the FW parts included in the evaluation.

The firmware has two parts:

- Metrological part
- Application part

Table 3 - Equivalency of SX601 and SX631

Type	Hardware version	Metrological FW version	Metrological FW Version CRC	Application FW version	Application FW Version CRC
SX601	S12U26 S15.Y4.J0 M12	V0.03.10	F289	E.S12U26.HU.007179.V1.00.33	3CD3
SX631	S34U28 S38.Y2.J0 M11	V0.10.10	A434	E.S34U28.HU.007178.V1.00.33	B3DC

A checksum generated with CRC16 is used to verify that the firmware version has not changed at startup.

Firmware integrity protection relies on two main measures:

1. Anti-tampering measures (see section 7.4.1);
2. Digital signature protected firmware updates (see section 7.6[1]).

For firmware upgrades the firmware package is always protected by a digital signature and an AES_GCM_128 tag.

The metrological part of the firmware is separated from all other firmware modules. The application part implements all the application functions except the functions in metrological area. For example, communication process, event log, display, tariff etc.

Due to the differences in the measurement part of the meters the underlying drivers of communication, events (three-phase L2L3 related events), display data items (three-phase L2L3 related objects, inconsistent underlying drivers), load profile, billing supported objects (L2L3), and instantaneous values (L2L3 part) are inconsistent.

On Figure 1: TOE Boundary a illustrates the TOE itself (highlighted with red bracket), its internal and external components, and the additional third-party firmware and hardware required for the operation of the TOE. The SANXING Smart Meter adopted advanced micro-electronics technology and SMT manufacturing process, according to corresponding national and international standards of EN 50470-1/3, IEC 62052-11, IEC 62053-21/22/23. The TOE has high accuracy, strong function, and good stability. The meter has four kinds of standard communication: optical, RS485, P1, and a replaceable module (GPRS/4G, LTE-M). The meter case is made of antistatic plastic (polycarbonate). The LCD display, ALT button, display button and optical port are always visible.

An AMI usually contains at least an intelligent measurement device, in our case smart meter, and a Head-End System (HES). The meter configuration tool Sanplat provided by the manufacturer has every functionality to replace a HES for the time of the evaluation and makes it possible to test every TOE related functionality of the TOE.

1.3.2 TOE Type

The smart meter was developed in accordance with the international standards of the advanced measurement infrastructure. These standards can be found in section 1.3 TOE Overview. The TOE is an electronic device that records and transmits information such as electrical energy consumption, voltage level, and current. Smart meters transmit information to the consumer and electricity providers for system monitoring and customer billing. The smart meter can be accessed remotely therefore the data can be accessed at any time by anyone who has the right to access it.

1.3.3 TOE Usage and Major Security Features

1.3.3.1 Local Data Security

[1] For firmware upgrades the firmware package is always protected by a digital signature and an AES_GCM_128 tag.

The meter has sealed screws to prevent unauthorized access and support serial device detections. After establishing the serial port connection signals exposed by the serial port can be set for device detection.

There are two different set of seal protection. First set protects terminal cover while the second protects meter cover. If seals are tampered with and either of the terminals is removed, then the corresponding events are recorded in the fraud event log. In case of terminal cover open, the dedicated counter (Cover opening counter) is incremented as well.

The following picture shows the structure of the TOE and the sealed screws:

Figure 3 - SX601

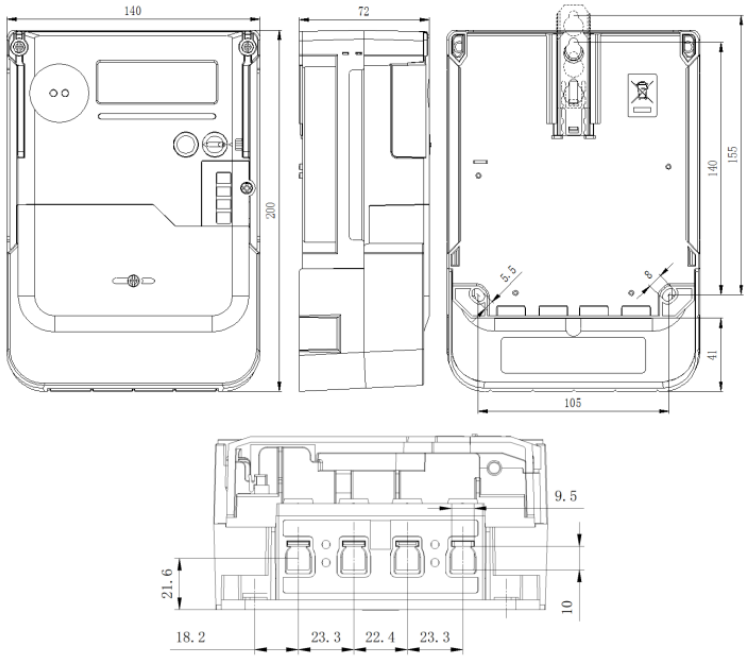
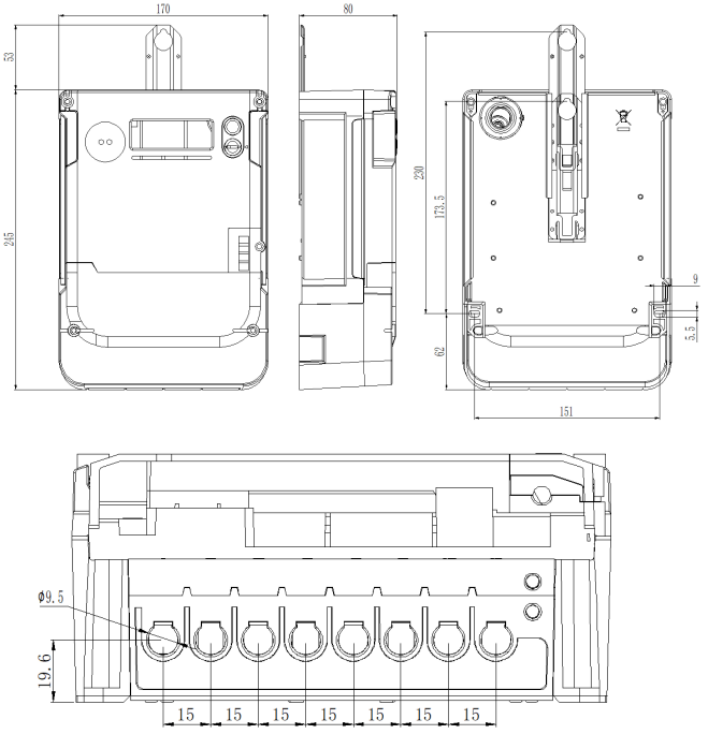


Figure 4 - SX631



1.3.3.2 Communication Security and security suite

The following table summarizes the ciphers provided by the TOE:

Table 4 – The used DLMS/Cosem security suite configurations

Security Suite ID	Suite name	Authenticated encryption	Digital signature	Key agreement	Hash	Key transport
0	AES-GCM	AES-GCM-128	-	-	-	AES key wrap 128 bit
1	ECDSA-AES-GCM-128-SHA-256	AES-GCM-128	ECDSA WITH P-256	-	SHA-256	AES key wrap 128 bit
2	ECDSA-AES-GCM-256-SHA-384	AES-GCM-256	ECDSA WITH P-384	-	SHA-384	AES key wrap 128 bit

Even though the TOE can work in the above-mentioned security suites, only Security Suite 0 is part of the evaluation.

The TOE will be delivered with unique passwords and keys to the customer, which will be loaded by the manufacturer. The common method is to use PGP encryption, before the transmission of the corresponding file, share their public keys with each other, and then decrypt with their private keys; The channel for transferring files can be via email, or can add security by setting up a dedicated VPN.

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.

The Manufacturer provides additional non-TOE software for parametrization of the TOE: Sanplat V.HU.11306.1.2, the software includes the following functionalities:

- Authentication and authorization: accessing the software needs username and password, different users can be configured with different rights by the service provider.
- Accessing the meter locally by its optical serial and P1 port or remotely through cellular communication.
- From the menu settings, parameters, commands, and the status of the communication is available.
- Reading data: cumulative energy per line, electricity related objects – instantaneous voltage, current, and power, and load profiles
- Alarms, log files
- Modem parameters – validating connections settings
- Tariff table

Additional non-TOE hardware required for communication with the TOE:

- Field exchangeable communication modules:
  - GPRS/4G
  - LTE-M
- IRDA serial converter, which conforms to [IEC 62056-21], for the optical (infrared) interface.
- P1 cable, which conforms to [IEC 62056-21], for P1 port RJ12 connector
- RS485 cable, which conforms to TIA/EIA EIA-485 -A [RS-485] and [IEC 62056-46] (HDLC)

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 task of the TOE is to measure and monitor energy parameters. After processing the data, forward it to the "Head-End-System". The end user can read the measured data using the LCD display on the TOE. The Head-End-System can connect back to the TOE and configure it, for example the current time.

The smart meter was developed in accordance with the international standards of the advanced measurement infrastructure. The following pictures show its construction:

Figure 5 - Main parts of SX601

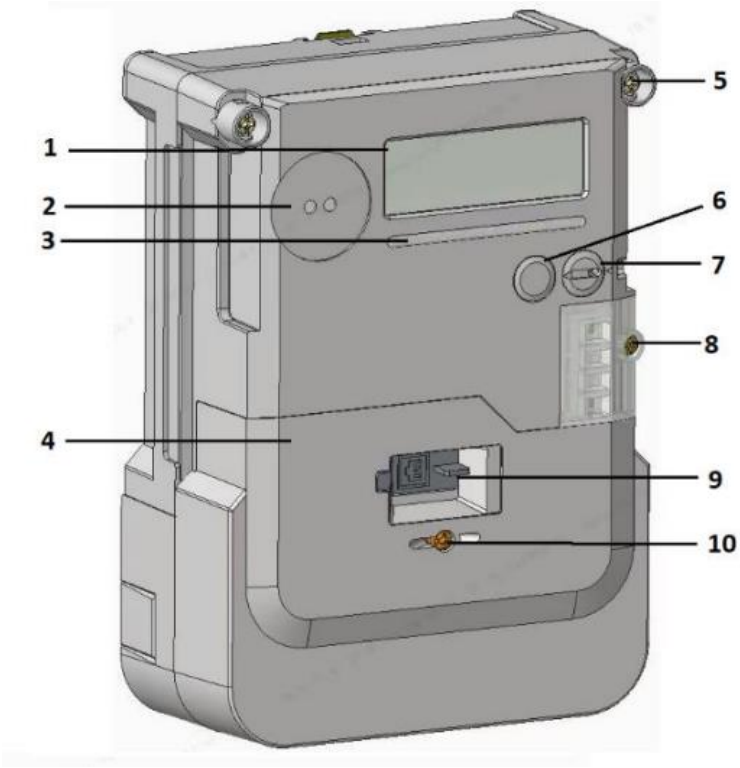
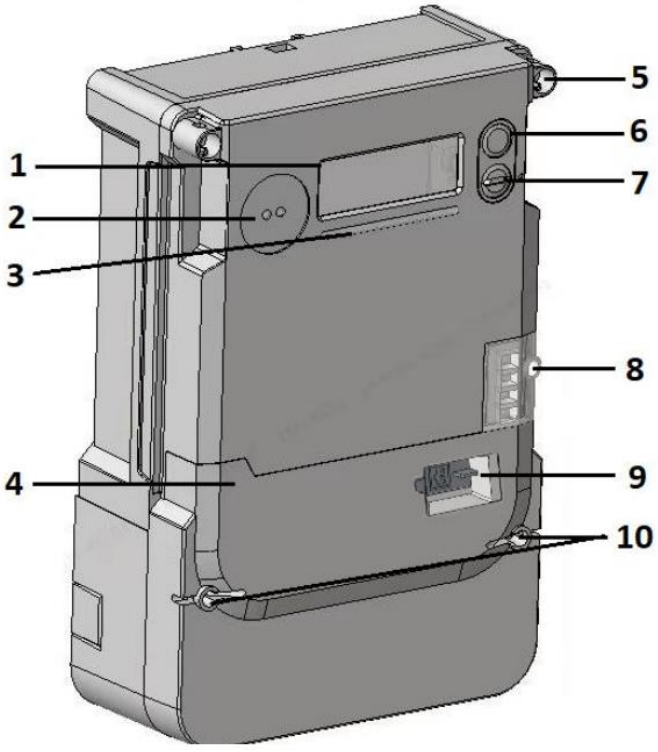


Figure 6 - Main parts of SX631



The numbering and associated parts of the two types are the same.

1. LCD display
2. Optical interface
3. LED interface
4. Terminal cover
5. Measuring cover screw
6. LCD Push button

7. Sealable push button
8. Module and module screw
9. P1 port
10. Terminal cover and screw

The TOE includes a meter hardware and a firmware. The two hardware with its parts can be found above (Figure 5 and 6).

The versions for each component can be found in Table 3. According to the version number in table 3, the corresponding firmware packages are:

- SX601: E.S12U26 S15.Y4.J0.HU.007179.47607.V1.9.zip
- SX631: E.S34U28 S38.Y2.J0.HU.007178.47609.V1.9.zip

The firmware part of the TOE is always preloaded to the meter before delivery, so every component of the TOE is delivered together.

1.4.2 Delivery of the TOE and documents

For the physical delivery of electricity meters, before delivery, the delivery parameters will be confirmed with the customer, such as what all the electricity meter parameters should be configured, how to package the electricity meter, what stickers are needed, the size of the packaging, the size of the pallet, etc., all the details. After reaching an agreement and confirmation with the customer, delivery will be carried out according to the demand via a courier delivery.

When the customer receives the product, physical and procedural checks can be done. The hardware acceptance procedures can be found in [AGD] section 3.1.1.

The documents or software upgrade packages will be delivered with unique passwords and keys to the customer. The firmware is always preloaded upon delivery.

The SHA-256 hash values corresponding to the delivered documents will be summarized in a table and sent to the customer. The customer will be able verify the integrity of the files through the corresponding hash value.

1.4.2.1 Guidance documents

- Smart Meter User Manual Model S12U26 [SX601]
- Smart Meter User Manual Model S34U28 [SX631]
- AGD Documentation SANXING Smart Meter (SX601 and SX631) [AGD]

1.4.3 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 not part of the evaluation, including:
  - Energy
  - Demand
  - Display
  - Instantaneous Measurement
  - Billing
  - Identification numbers
  - TOU

    - Load Profile
    - Relay
    - Load Management-Relay control
- Functions in the logical scope of the evaluation
    - Clock and Calendar
    - Event Record
    - Errors and Alarms
    - Security
    - Push
    - Firmware upgrade
- Meter communication functions, including network interfaces and direct interfaces
    - Optical Port
    - RS485
    - Communication Module
        - GPRS/4G module
        - LTE-M module
    - P1 Port

1.4.3.1 Clock and Calendar

This IC models the device clock, managing all information related to date and time including deviations of the local time to a generalized time reference (UTC) due to time zones and daylight-saving time schemes. The IC also offers various methods to adjust the clock.

The date information includes the elements year, month, day of month and day of week. The time information includes the elements hour, minutes, seconds, hundredths of seconds, and the deviation of the local time from UTC. The daylight-saving time function modifies the deviation of local time to UTC depending on the attributes.

1.4.3.2 Event Record

Events are generated by the meter itself or by its environment. All these events are logged in several event logs. Every event has a unique code to identify the action which has triggered it. Every event (except Event log cleared) is assigned to one event log and it is only stored there.

The TOE features the following event log type:

- Standard event log
- Fraud detection log
- Disconnector control log
- Power quality event log
- Communication event log
- Phase interruption log
- Output Control K1 log
- Image activate log
- Security event log
- Power failure event log

The TOE features the following event log objects:

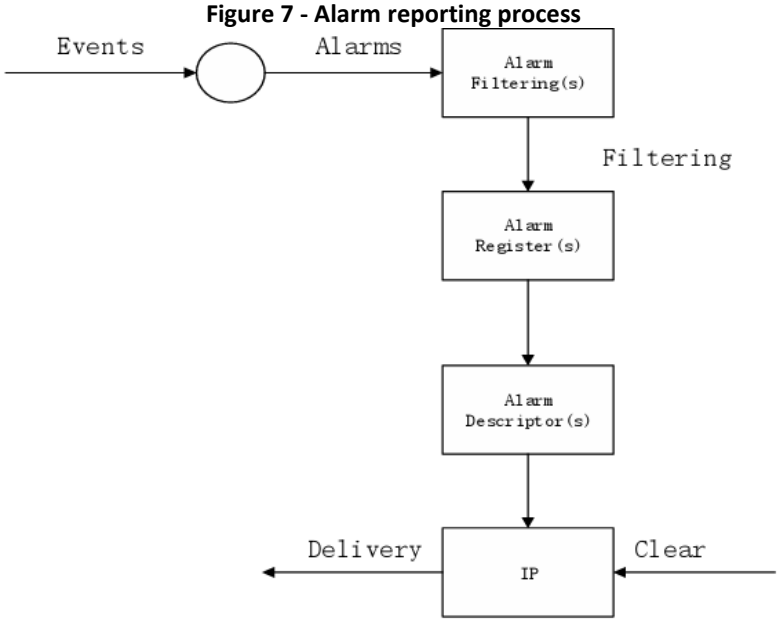
Table 5 – Event log objects

Event log object	Logical Name	Captured Objects
Standard event log	0-0:99.98.0.255	0-0:1.0.0.255 0-0:96.11.0.255
Fraud detection log	0-0:99.98.1.255	0-0:1.0.0.255 0-0:96.11.1.255
Disconnector control log	0-0:99.98.2.255	0-0:1.0.0.255 0-0:96.11.2.255
Power quality event log	0-0:99.98.4.255	0-0:1.0.0.255 0-0:96.11.4.255
Communication event log	0-0:99.98.5.255	0-0:1.0.0.255 0-0:96.11.6.255
Phase interruption log	1-0:99.97.1.255	0-0:1.0.0.255 0-0:96.11.7.255
Output Control K1 log	0-0:99.98.20.255	0-0:1.0.0.255 0-0:96.11.20.255
Image activate log	0-0:99.98.22.255	0-0:1.0.0.255 0-0:96.11.12.255
Security event log	0-0:99.98.26.255	0-0:1.0.0.255 0-0:96.11.26.255
Power failure event log	1-0:99.97.0.255	0.0.96.7.10.255 0.0.96.7.15.255

1.4.3.3 Errors and Alarms

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.

Figure 7 - Alarm reporting process



1.4.3.4 Security

E-meter security is devised into Physical Security and Logical Security.

The physical security is a traditional way of protecting E-meter from different tampering variants and unauthorized access.

With increase of smart meter numbers and the rise of AMI infrastructures, the logical security was introduced in E-meters.

Therefore, the TOE is provided with both logical and physical security. TOE has tamper protection. If anyone tries to disassemble the TOE, TOE can send a signal to the HES about the tamper status.

DLMS communication needs authentication first. AA successfully establishes the link and enters the application layer. After the application layer passes the authentication (such as decryption authentication) according to the security policy communication security requirements, it verifies the OBIS authority according to the OBIS authority meter of each client. After passing, the meter operates the operation requirements of the client. If there is a broken link frame, the link is broken according to the security requirements of the link-building frame. If it does not meet the security requirements of the link-building frame, the link is continuously broken.

1.4.3.5 Push

PUSH data format is in accordance with Data-Notification. Push has the following functions:

- All Push objects can be set remotely and locally. The push object is no limit.
- All Push parameter (such as randomisation_start_interval, number_of_retries, repetition_delay) can be set separately through remote and local.
- The unfinished Push before power failure can be reported after power on again
- Interval 1, Interval 2, Interval 3 and Consumer Information support 4 groups of time and date.

1.4.3.6 Firmware upgrade

Updating the firmware is important for the optimal functioning of TOE. The latest firmware versions ensure more efficient and secure operation of TOE.

E-Meter and Communication module upgrade features are as follows:

- Support broadcast upgrade and point-to-point upgrade.
- Support continuous upgrade after communication interruption.
- If some upgrade packages fail to be transmitted, supplementary transmission of these upgrade packages is supported.
- Support locally and remotely

1.4.3.7 Communication

TOE uses network interfaces for communication. It has ports that must relate to a physical cable, but it also has a GSM module. The TOE has the following ports:

- Optical Port
- RS485
- Communication Module
    - GPRS/4G module
    - LTE-M module
- P1 Port

1.5 Non-TOE functions

1.5.1.1 Energy

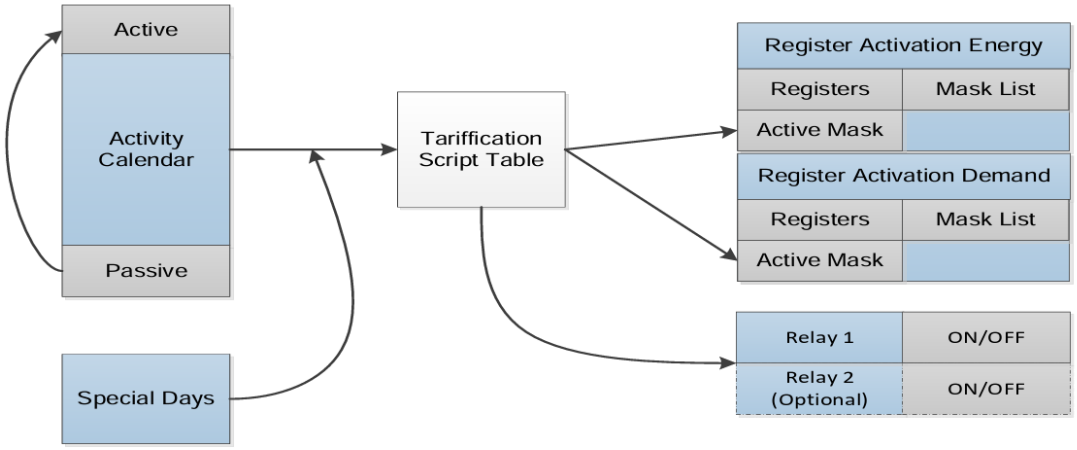
Electrical meter energy is accumulated in respective registers (A+ or A-) until 1 Wh is reached thus energy measurement is carried out in latter unit. Nevertheless, full value with each Wh counted could be obtained through communication interfaces in form of value, unit and scaler.

The measurement system is calibrated during the manufacturing process of the meter. Calibration data is stored in a non-volatile (EEPROM) memory and cannot be altered.

1.5.1.2 TOU

Tariff program is implemented with set of objects that are used to configure different seasons or weekly and daily programs, to define which certain tariffs should be active. Also, different actions can be performed with tariff switching like for example registering energy values in different tariffs or switching on/off bi-stable relay. Graphical tariff program illustration can be seen on figure below.

Figure 8- TOU



Tariff program configures different seasons or weekly and daily programs to define, which certain tariffs should be active. Different actions can be performed with tariff switching like registering energy values in different tariffs or switching on and off the bi-stable relay.

1.5.1.3 Load profile

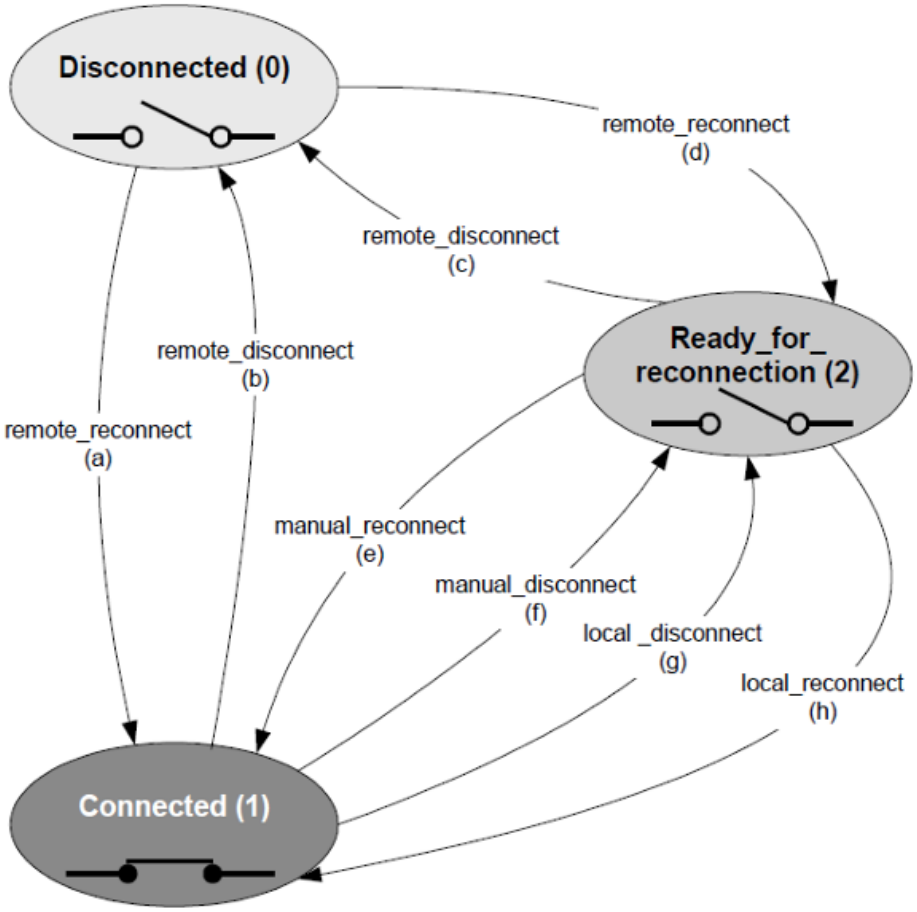
Three general purpose load profiles are available in meter. Each of two can capture any of the basic type of object value present in the meter. Basic object type means any object attribute that has non structured content.

The meter has two load profiles (LP with period 1 and LP with period 2) which are instances of the COSEM class the "Profile generic", which defines a generalized concept to store dynamic process values of capture objects. A profile has a buffer to store captured data; therefore, each profile has a limit of stored data. More capture objects we select less total captured data will be possible to store.

1.5.1.4 Relay

The DC meter has a built-in relay to control the reconnection or disconnection of electric network to individual customers. The relay can be performed remotely, locally, and manually. The CT meter has no built-in relay.

Figure 9 - Relay



1.5.1.5 Load Management-Relay control

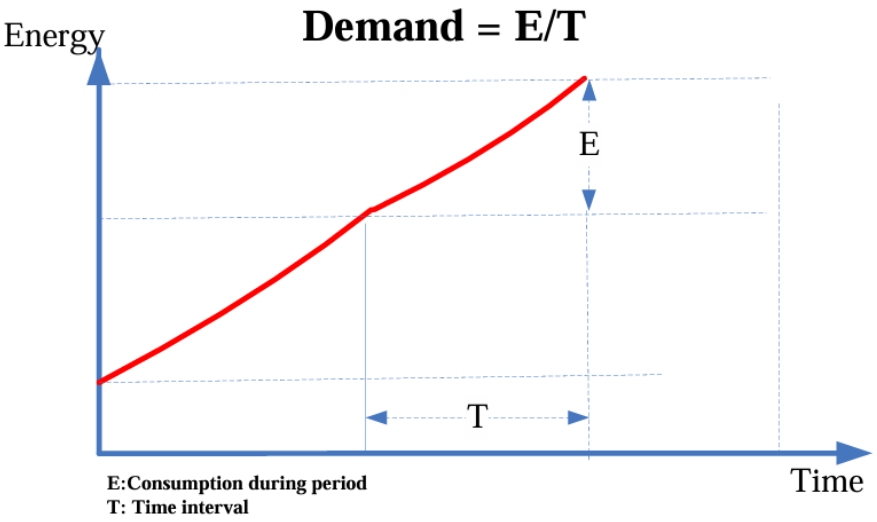
The relay is a device that can indirectly control high voltage and strong current through the on and off low voltage and weak current circuits.

The states and state transitions of the Relay control are described in 1.4.3.9 Relay section. The possible state transitions depend on the control mode. To define the behaviour of the disconnect control object for each trigger, the control mode shall be set.

1.5.1.6 Demand

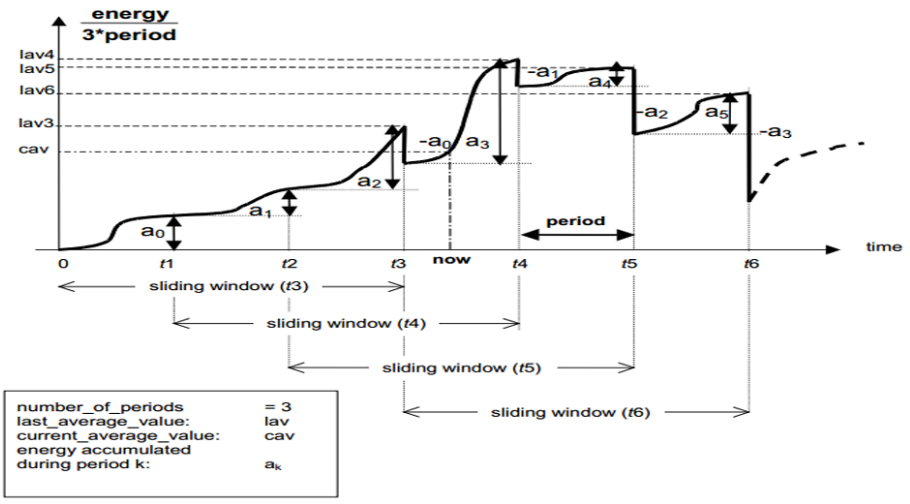
Meter calculates an average demand in a time interval. Where Time Interval =period*number_of_periods.Both period and number_of_periods are configurable.

Figure 10- Demand Definition



Assuming that the demand period is 5 min, it will not be measured until the integer multiple of the demand cycle (for example 01, 10, 01, 15, which is an integer multiple of 5), and the amount required in other places will remain unchanged. The sliding period which the sliding average value is calculated is defined by specifying number_of_periods and period.

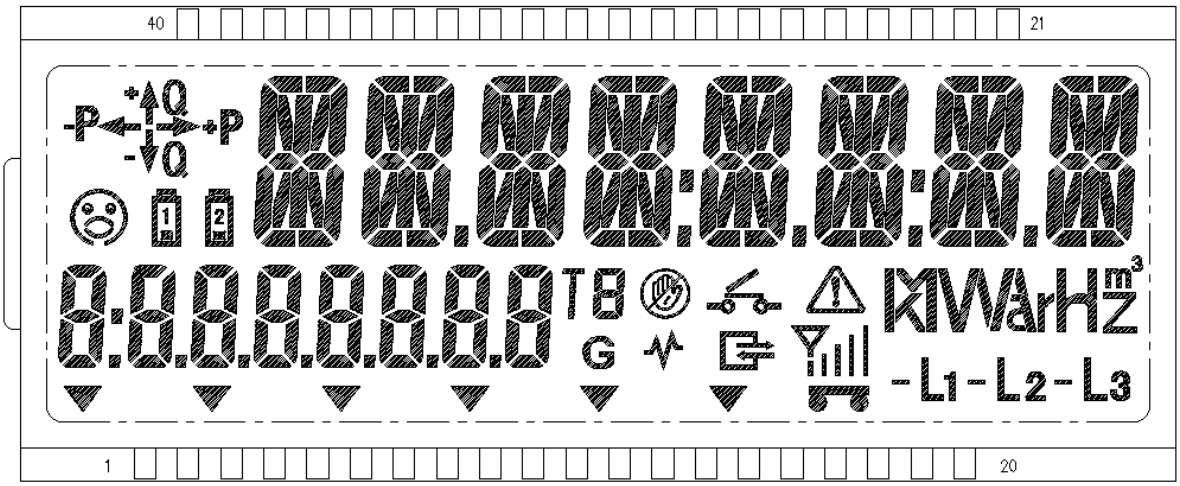
Figure 11- Sliding demand type



1.5.1.7 Display

The TOE has a one integrated display. The display is a seven-segment liquid crystal display (LCD) complies with the VDEW requirements. The TOE data and the state of the status registers can be read on the display. The data reading can be progressed with the push button on the TOE. The status registers are continuous lighting or flashing on the display. The structure of the display is as follows:

Figure 12- seven-segment liquid crystal display (LCD)



The meter has two objects, which can be configured with auto display and other display format. It supports that decimal and leading zero can be configured such as energy, demand, voltage, current, power, power factor, frequency, and angle.

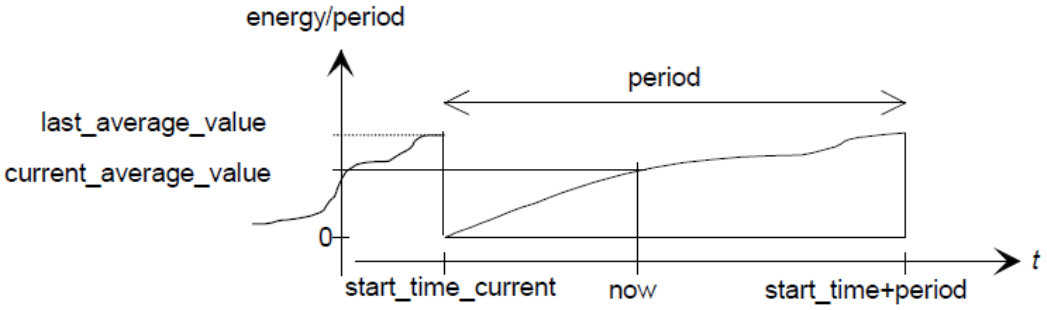
1.5.1.8 Instantaneous Measurement

Support the measurement of instantaneous value, interval average value, sliding average value and maximum and minimum value.

Interval period can be set 60s, 120s, 180s, 240s, 300s, 360s, 600s, 720s, 900s, 1200s, 1800s, 3600s. Interval average value and maximum and minimum value refresh when cycle arrives.

Update data every Interval period. When the period is changed, the last Interval average value will be retained. Then it will restart and be updated when the new Interval period arrives.

Figure 13 - Interval average value calculation



1.5.1.9 Billing

The energy providers bill the end user for the energy used. The billing process is based on the TOU.

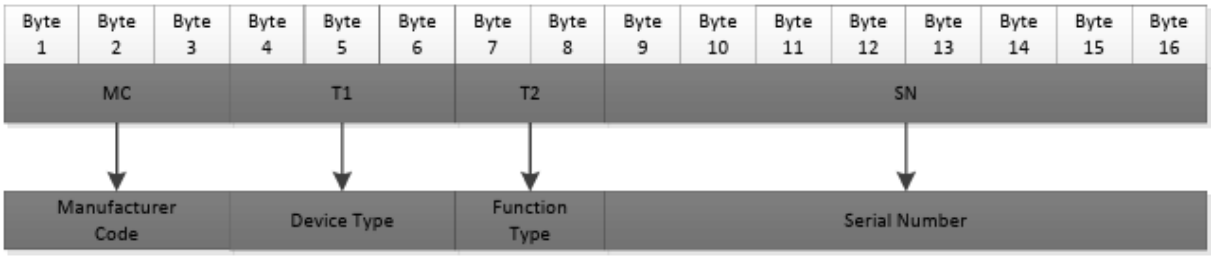
1.5.1.10 Identification numbers

The COSEM logical device can be identified by its unique COSEM logical device name. This name can be retrieved from an instance of IC "SAP assignment", or from a COSEM object

named "COSEM logical device name". The name is of type octet-string of up to 16 octets in size.

The following figure presents the division of the "COSEM logical device name" as enforced by the IDIS association:

Figure 14 - Definition of COSEM logical device name



2 Conformance Claims

Table 6 - 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:

- Assets
- Secure Usage Assumptions,
- Threats, and
- Organisational Security Policies (OSPs).

3.1 Assets

R.MeterData: The measurement data, and the actual state of the meter.

R.ConfigurationData: The configuration parameters and settings stored by the meter.

R.EventRecords: The meter creates a log record for every event (Standard Event Log, Fraud Detection Log, Disconnector Control log, Power Quality log, Communication event log, Power failure event log, Phase interruption log, Output Control K1 log, Image active event log, Security event log).

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

R.AuthKeys: There are six access levels supported with different keys: management, technician, reader, pre-established, public, upgrade. Each access level has different authentication keys.

R.GlobalUnicastKey: It is used to cipher and decipher every unicast DLMS frame, AES_GCM crypt algorithm will be used for the below DLMS message:

- Initiate Request, Initiate Response in AARQ, AARE, RLRQ, RLRE
- GET, SET, ACTION Requests and Responses and DataNotification

R.LLSKey: LLS key is used to authenticate the reader client is initiate a establish request:

- AARQ

R.GlobalBroadcastKey: GBEK is used to cipher and decipher every broadcast DLMS frame, AES_GCM crypt algorithm will be used for the below DLMS message:

- GET, SET, ACTION Requests and Responses

R.KeyEncryptionKey: it is also called the key encrypt key, it is used to wrap and unwrap other keys to be set when security setup is executing to protect the key being set in a ciphertext, AES key wrap algorithm will be used for the below DLMS message:

- ACTION Requests of security setup

R.FirmwareDecryptionKey: The Firmware decryption key is used to decrypt the newly received firmware binary file when it is in a firmware upgrade process. AES_ECB crypt algorithm will be used for meter firmware file decryption.

3.2 Assumptions

Table 7 - 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.
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].)

3.3 Threats

3.3.1 T.NetworkDisclosure Unauthorised data disclosure via network access

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

3.3.2 T.DirectDisclosure Unauthorised data disclosure via direct access

An attacker gains access to data that requires protection of confidentiality (defined according to the policies implemented in the TOE, as described for T.NetworkDisclosure).

Access might be gained either from intercepting messages in transit to or from the TOE, or by executing a command (without authorisation) via a direct interface to access data stored in the TOE (noting that, in additional to any network interfaces a direct attacker will also be able to use any other interfaces present on the meter, such as the display and keypad). In addition, the attacker might attempt unauthorised physical access to the meter by accessing internal interfaces and components (e.g., to access memory directly, without using the intended interfaces).

3.3.3 T.NetworkDataMod Unauthorised data modification via network access

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

3.3.4 T.DirectDataMod Unauthorised data modification via direct access

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

3.3.5 T.Malfunction Asset compromise due to TOE malfunction

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

3.4 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 8 - 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[2].

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 9 - 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 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**

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

	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 10 - 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 tables 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 11 – 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.InspectionSupport	OE.UniqueSubjectIDs
T.NetworkDisclosure	X	X	X	X	X									
T.DirectDisclosure	X	X	X	X	X								X	
T.NetworkDataMod	X	X	X	X	X									

T.DirectDataMod	X	X	X	X	X								X	
T.Malfunction					X	X	X							
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[3].
- 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 3.2 is directly matched by a security objective for the operational environment in section 4.1.1 Table 11. 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

[3] 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.

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

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*].

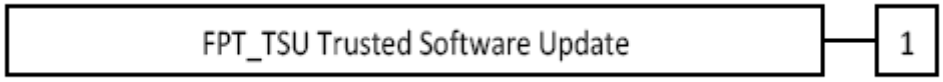
FAU_ARP.2.4 The TSF shall send alarms according to the following timing rules: [assignment: *rules that specify when an alarm must be sent relative to the detection of the event*].

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

FPT_TSU.1	*Trusted Software/Firmware Update*

There are no actions defined to be auditable by default.

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.

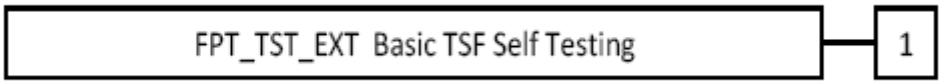
If the TOE does not support the querying of the currently executing version, then it is legitimate to complete the assignment of the list of roles in FPT_TSU.1.1 with 'None', and in this case the SFR element is treated as trivially satisfied.

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.



Note: The ST author used the image from the protection profile [SM-MSR] to be compliant with it.

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

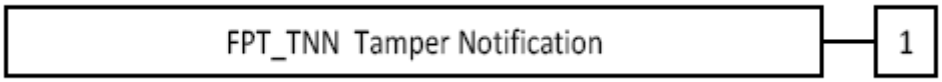
FPT_BST.1.1 The TSF shall run a suite of the following self-tests [selection: during initial start-up (on power on), periodically during normal operation, the request of the authorised user, at the conditions [assignment: *conditions under which self-tests should occur*]] to demonstrate the correct operation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

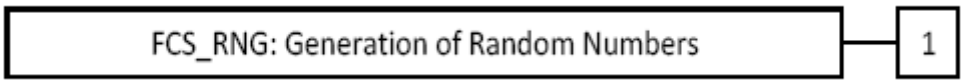
Application Note 8 (Application Note 8 from [SM-MSR])

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 15 - Architecture of Message Security, TSF Protection and Audit SFRs and Figure 17 - Architecture of Data Protection and Underlying Cryptography SFRs give a graphical presentation of the connections between the Security Functional Requirements (SFRs) from section 6.4 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 6.4 defines the SFRs grouped by the abstract class and family groupings in [CC_P2].

Figure 15 - Architecture of Message Security, TSF Protection and Audit SFRs

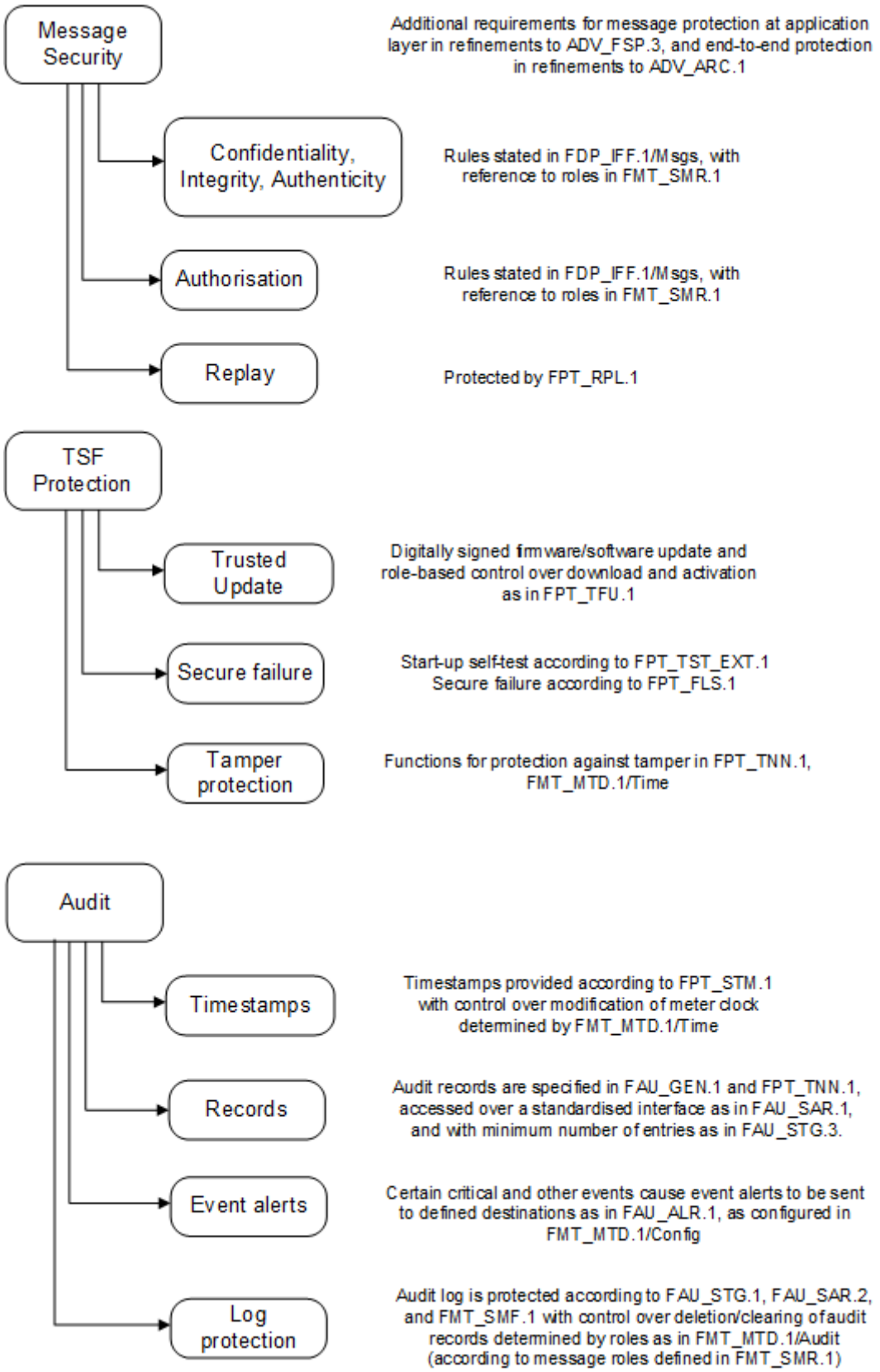


Figure 16 - Architecture of Authentication & Authorisation SFRs

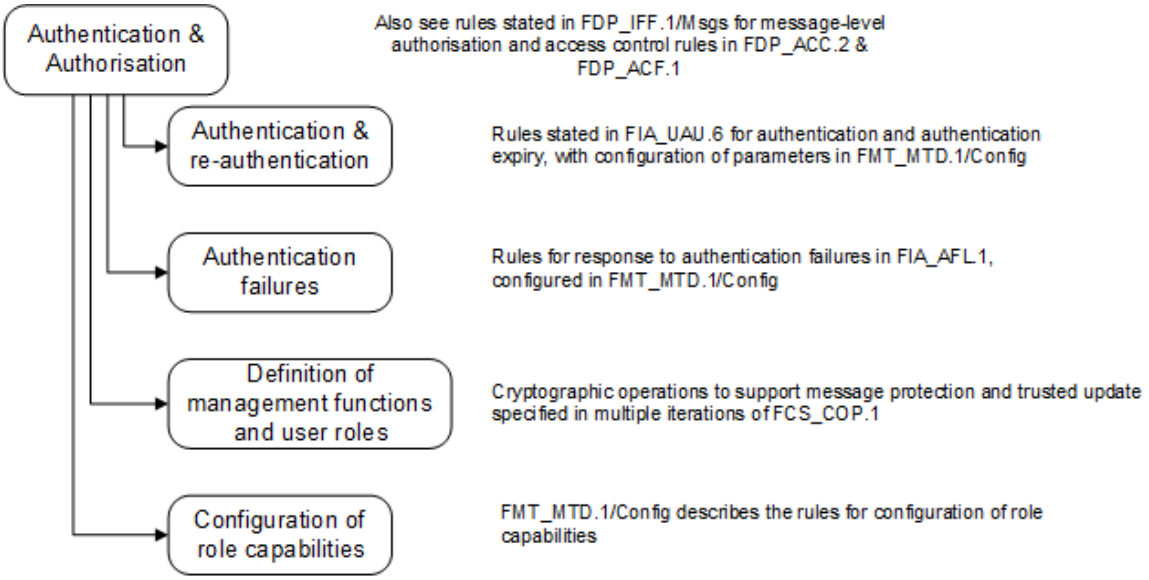
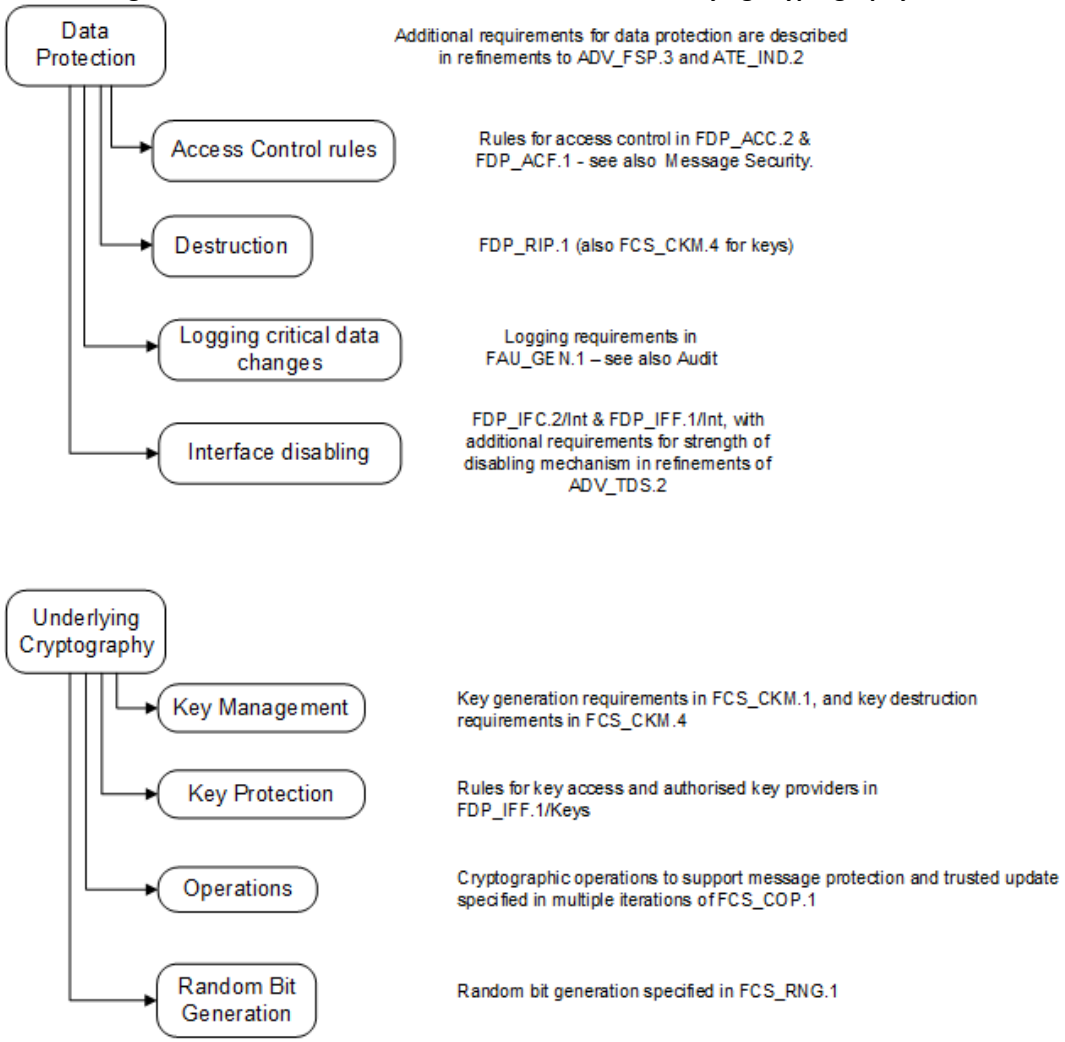


Figure 17 - Architecture of Data Protection and Underlying Cryptography SFRs



6.3 TOE Security Functional Requirements

Table 12 - SFRs

Name	Description	S	A	R	I
FCS_CKM.1	Cryptographic key generation		x		
FCS_CKM.4	Cryptographic key destruction		x		
FCS_COP.1/KE	Cryptographic operation – Key Encryption		x		
FCS_COP.1/GUE	Cryptographic operation – Global Unicast Encryption		x		
FCS_COP.1/GBE	Cryptographic operation – Global Broadcast Encryption		x		
FCS_COP.1/Auth	Cryptographic operation – Authentication		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 [*None*] [4] and specified cryptographic key sizes [*None*][5] that meet the following: [*None*][6].

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).

Application Note from the ST author 1

The TOE does not generate any keys. Because there are no key generation in the TOE the FCS_CKM.1.1 was removed from the security requirements and the dependencies connected to this SFR are trivially fulfilled.

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 [*the meter will always contain one set of keys, and the keys can be replaced only by overwriting with a new set of keys*][7] that meets the following: [*B-Book*][8].

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

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

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

6.3.1.3 Cryptographic operation (FCS_COP.1) – Key Encryption

FCS_COP.1/KE	*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/KE The TSF shall perform [*wrap and unwrap other keys to be set*][9] in accordance with a specified cryptographic algorithm [*AES key wrap*][10] and cryptographic key sizes [*128*][11] that meet the following: [*[FIPS PUB 197]*][12].

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.

6.3.1.4 Cryptographic operation (FCS_COP.1) – Global Unicast Encryption

FCS_COP.1/GUE	*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/GUE The TSF shall perform [*symmetric encryption and decryption of unicast DLMS frames*][13] in accordance with a specified cryptographic

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

algorithm [*AES-GCM*][14] and cryptographic key sizes [*128*][15] that meet the following: [*FIPS PUB 197:2001*][16].

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.

6.3.1.5 Cryptographic operation (FCS_COP.1) – Global broadcast encryption

FCS_COP.1/GBE	*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/GBE The TSF shall perform [*symmetric encryption and decryption of broadcast DLMS frames*] [17] in accordance with a specified cryptographic algorithm [*AES-GCM*][18] and cryptographic key sizes [*128*][19] that meet the following: [*FIPS PUB 197:2001*][20].

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.

6.3.1.6 Cryptographic operation (FCS_COP.1) - Authentication

FCS_COP.1/Auth	*Cryptographic operation*

[14] [assignment: *cryptographic algorithm*]
[15] [assignment: *cryptographic key sizes*]
[16] [assignment: *list of standards*]
[17] [assignment: *list of cryptographic operations*]
[18] [assignment: *cryptographic algorithm*]
[19] [assignment: *cryptographic key sizes*]
[20] [assignment: *list of standards*]

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/Auth	The TSF shall perform [*authentication of every DLMS frame and verify its integrity by symmetric encryption*][21] in accordance with a specified cryptographic algorithm [*AES-GCM*][22] and cryptographic key sizes [*128*][23] that meet the following: [*FIPS PUB 197:2001*][24].

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.

6.3.1.7 Cryptographic operation (FCS_COP.1) – Firmware Decryption

FCS_COP.1/FW	*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/FW	The TSF shall perform [*decryption the new received firmware binary file during the firmware upgrade process*][25] in accordance with a specified cryptographic algorithm [*AES_ECB*][26] and cryptographic key sizes [*128*][27] that meet the following: [*FIPS PUB 197:2001*][28].

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

[21] [assignment: *list of cryptographic operations*]
[22] [assignment: *cryptographic algorithm*]
[23] [assignment: *cryptographic key sizes*]
[24] [assignment: *list of standards*]
[25] [assignment: *list of cryptographic operations*]
[26] [assignment: *cryptographic algorithm*]
[27] [assignment: *cryptographic key sizes*]
[28] [assignment: *list of standards*]

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.

6.3.1.8 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 [deterministic][29] random number generator that implements: [*HLS5 (PRNG for AARE 8*32bit)*][30].

FCS_RNG.1.2 The TSF shall provide [bits][31] that meet [*CAVP validated*[32]][33].

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*[34] on

(1) subjects: all

(2)objects: metrologically certified data, credentials, meter configuration, [*log records, alarms*][35]

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])

---

[29] [selection: physical, deterministic, hybrid physical, hybrid deterministic]
[30] [assignment: *list of security capabilities*]
[31] [selection: bits, octets of bits, numbers [assignment: *format of the numbers*]]
[32] https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?validation=35435
[33] [assignment: *a defined quality metric*]
[34] [assignment: *access control SFP*]
[35] [assignment: *list of subjects and objects*, [*assignment*: *other controlled meter data items*]]

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

6.3.2.2 Security attribute-based access control (FDP_ACF.1)

FDP_ACF.1	*Security attribute-based access control*

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the *Meter Data SFP*[36] to objects based on the following:

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

(2) Credentials

(3) Meter configuration

(4) [*None*][37]

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: [

(1) public: read basic info cannot read and write any other data,

(2) reader client: can only read the measurements data and configuration of the meter,

(3) management client: can read the measurements data, read and write the configuration of the meter,

(4) technician client: default cannot update the keys and others the same as management, can be modified at the factory according to customer requirements,

[36] [assignment: *access control SFP*]
[37] [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,* [*assignment: list other 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*]]

(5) *pre-established client: default write some config, can be modified at the factory according to customer requirements, and report data(push) to the HES*

(6) *upgrade: Used only for meter or module FW upgrade*

]38.

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules:[*Each object/data with access_mode for each client, meter will check the client with right to access the object or not, access_mode define as bellow:*
access_mode: enum {Bit attribute access_mode

- *(0) read access*
- *(1) write access*

}]39.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*If the client read or write the object without access right or without allowed security is reject.*]40.

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.

Application Note from the ST author 2

Even though in [SM-MSR] section 6.4.1.4 Architectural Design (ADV_TDS.2), the second refinement requires that all operational interfaces should be subject to the requirements of FDP_ACF.1, FDP_IFF.1/Msgs and FDP_IFF.1/Keys, P1 port is an exception from this. Due the physical and logical design of the interface ([DSMR-P1]) the interface does not provide role or security attribute-based access control, no keys are required. The receiving pin (RX) is missing physically from the connector, so the meter cannot receive any messages on that interface, only the configured information is sent periodically through its transmitter pin (TX).

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*41 on

38 [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
39 [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
40 [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

(1) subjects: all

(2) information: messages

(3) operations: send, receive[42].

6.3.2.4 Simple security attributes (FDP_IFF.1) – Messages

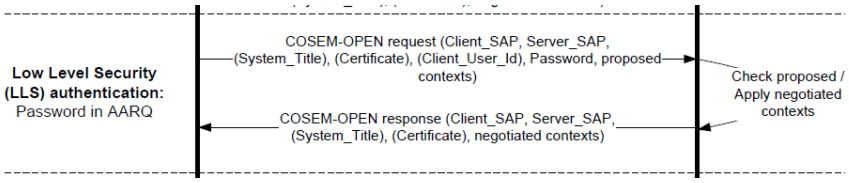
FDP_IFF.1/Msgs	*Simple security attributes*

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

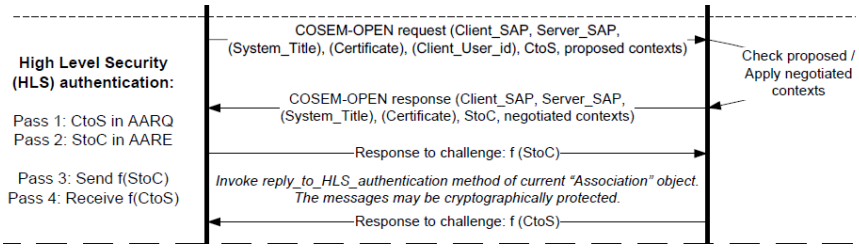
FDP_IFF.1.1/Msgs The TSF shall enforce the *Messages SFP*[43] based on the following types of subject and information security attributes: [*establish association (LLS, HLS), read, write, action, service-specific ciphering, General glo-ded ciphering, general signing, general block transfer(only for push); disconnect association*][44].

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) establish association: LLS-the messages format must comply with DLMS UA 1000-2([G-Book]), the client_SAP and Server_SAP must allow by the meter, the password must correct. The process as bellow:



(2) establish association: HLS-the messages format must comply with DLMS UA 1000-2([G-Book]), the clientSAP and Server_SAP must allow by the meter, the F(StoC)&F(CtoS) GMAC. the process as bellow:



---

[41] [assignment: *information flow control SFP*]
[42] [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*]
[43] [assignment: *information flow control SFP*]
[44] [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]

Table 13 - Authentication mechanisms

Authentication mechanism	Pass1	Pass2	Pass3	Pass4
HLS5 (GMAC)	CtoS: Random string 8-64 octet; System-Title-C;	StoC: Random string 8-64 octets; System-Title-S;	SC II IC II GMAC (SC||AK|| StoC)	SC II IC II GMAC (SC||AK|| CtoS)

(3) service-specific ciphering: the AES-GCM-128 for protection

(4) General glo-ded ciphering: the AES-GCM-128 for protection

(5) general block transfer (only for push): the same as General glo- ciphering

(6) disconnect association: the protect method of user-information must the same as user-information of establish association

]45.

FDP_IFF.1.3/Msgs The TSF shall enforce the **following additional information flow control rules**46: [

(1) The messages protect by AES-GCM-128 with additional information is security control word (1 byte), AK (128 bit), and message (APDU data) when protect method is authenticated only.

(2) The messages protect by AES-GCM-128 with additional information is security control word (1byte), AK(128 bit) when protect method is authenticate and encryption.

]47.

FDP_IFF.1.4/Msgs The TSF shall explicitly authorise an information flow based on the following rules: [

(1) Replay check (frame counter in the message)

(2) Integrity and authenticity, access right validation (valid keys and ciphering)

]48.

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.

---

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

46 This refinement is applied to improve readability of the SFR element.

47 [assignment: *additional information flow control SFP rules*]

48 [assignment: *rules, based on security attributes, that explicitly authorise information flows*]

(2) [*service-specific ciphering, Frame counter in the message less than or equal to the frame counter in meter; the protect method lower than the configure (policy) of meter; Without establish association, expect the pre-established client*][49].

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.

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

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

of the interfaces. At the level of direct interfaces this would include interfaces such as using inter-PAN on a ZigBee TOE to communicate directly with a device such as a hand-held terminal unit.

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

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

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

Where the protection of messages is based on a secure channel rather than by protecting each individual message (noting that security measures are required to be implemented at the application layer and not to depend on the lower layer protocols, as checked in the refinements to ADV_FSP.3 in section 6.4.1.3 of [SM-MSR]) 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.

Application Note from the ST author 3

Even though in [SM-MSR] section 6.4.1.4 Architectural Design (ADV_TDS.2), the second refinement requires that all operational interfaces should be subject to the requirements of FDP_ACF.1, FDP_IFF.1/Msgs and FDP_IFF.1/Keys, P1 port is an exception from this. Due the physical and logical design of the interface ([DSMR-P1]) the interface does not provide role or security attribute-based access control, no keys are required. The receiving pin (RX) is missing physically from the connector, so the meter cannot receive any messages on that interface, only the configured information is sent periodically through its transmitter pin (TX).

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*[50] on
	(1) subjects: all

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

(2) information: all communication[51]

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*[52] based on the following types of subject and information security attributes: [*optical interface, RS-485, P1 interface, communication module*][53].

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***[54]: [*optical interface and RS-485 for on-site reading and parametrization, P1 interface for on-site reading (read only interface), communication module (GPRS/4G, LTE-M) for remote reading and parametrization of the TOE*][55].

FDP_IFF.1.3/Int The TSF shall enforce the **following additional information flow control rules**[56]: [*None]*[57].

FDP_IFF.1.4/Int The TSF shall explicitly authorise an information flow based on the following rules: [*None]*[58].

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[59].

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

[51] [assignment: *list of subjects and information*]
[52] [assignment: *information flow control SFP*]
[53] [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]
[54] if the following rules hold
[55] [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]
[56] This refinement is applied to improve readability of the SFR element.
[57] [assignment: *additional information flow control SFP rules*]
[58] [assignment: *rules, based on security attributes, that explicitly authorise information flows*]
[59] [assignment: *rules, based on security attributes, that explicitly deny information flows*]

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.

Application Note from the ST author 4

Even though in [SM-MSR] section 6.4.1.4 Architectural Design (ADV_TDS.2), the second refinement requires that all operational interfaces should be subject to the requirements of FDP_ACF.1, FDP_IFF.1/Msgs and FDP_IFF.1/Keys, P1 port is an exception from this. Due the physical and logical design of the interface ([DSMR-P1]) the interface does not provide role or security attribute based access control, no keys are required. The receiving pin (RX) is missing physically from the connector, so the meter cannot receive any messages on that interface, only the configured information is sent periodically through its transmitter pin (TX).

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*[60] on

(1) subjects: all

(2) information: keys

(3) operations: send, import[61]

6.3.2.8 Simple security attributes (FDP_IFF.1) – Keys

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

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

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

(1) Master key (MK): a cryptographic key that is used for the encryption or decryption of other keys,

(2) Global Unicast Encryption Key (GUEK): the Key for AES-GCM-128 when the security control word bit6=0 Unicast,

(3) Global broadcast key(GBEK): the Key for AES-GCM-128 when the security control word bit 6=1 broadcast,

(4) Authentication key(AK): additional information for AES-GCM-128 when protect method is authenticate only or authenticate and encryption,

]*[63]*.

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) MK, GUEK, GBEK, AK be change by RFC 3394 (Advanced Encryption Standard (AES) Key Wrap Algorithm), and MK is the key encryption key.

][64].

FDP_IFF.1.3/Keys The TSF shall enforce the **following additional information flow control rules**[65]: [*None*][66].

FDP_IFF.1.4/Keys The TSF shall explicitly authorise an information flow based on the following rules: [*None*] [67].

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.

---

[62] [assignment: *information flow control SFP*]
[63] [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]
[64] [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]
[65] This refinement is applied to improve readability of the SFR element.
[66] [assignment: *additional information flow control SFP rules*]
[67] [assignment: *rules, based on security attributes, that explicitly authorise information flows*]

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

(3) *[MK, GUEK, GBEK, AK: The key length does not match the configuration of meter, suite 0 must be 16 bytes (128bit).]*[68]

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).

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.

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

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*[69] the following objects: [*the meter will always contain one set of keys and only can be replaced by overwrite with a new key, the previous keys will no longer hold on the meter after the overwrite.*][70]

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**[71] the user **for access to data** under the conditions [*defined in the Re-authentication Table*][72].

Table 14 - Re-authentication Table

ID	Data	Authentication for initial access	Re-authentication
(i)	*[Metrologically certified data]*	[*encrypted and authenticated*]	*After a period of [every access to data] from the previous successful authentication*
(ii)	*[Meter configuration]*	*[encrypted and authenticated]*	*After a period of [every access to data] 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).

[69] [selection: allocation of the resource to, deallocation of the resource from]
[70] [assignment: *list of objects*]
[71] re-authenticate
[72] [assignment: *list of conditions under which re-authentication is required*]

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*[73] **of** unsuccessful authentication attempts occur related to *consecutive failed authentication attempts for access to protected data objects*[74].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *surpassed*[75], the TSF shall *block access for that entity via the relevant interface to data requiring prior authentication until the time period shown in the Authentication Failure Handling Table has elapsed*[76].

Table 15 - Authentication Failure Handling Table

ID	Type of authentication	Allowed range of authentication failures	Blocked time period
(i)	*[encrypted and authenticated]*	*[default 5 times(can configure)]*	*[1 min(can configure)]*

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 Basic TSF Self Testing (FPT_BST.1)

FPT_BST.1	*Basic TSF Self Testing*

Dependencies: No dependencies.

[73] [selection: [assignment: *positive integer number*], an administrator configurable positive integer within [assignment: *range of acceptable values*]]
[74] [assignment: *list of authentication events*]
[75] [selection: met, surpassed]
[76] [assignment: *list of actions*]

FPT_BST.1.1 The TSF shall run a suite of the following self-tests [during initial start-up (on power on), on reset][77] to demonstrate the correct operation of the TSF:

(1) Firmware integrity test

(2) Random bit generator test

(3) Correct TSF start-up

(4) [*None*][78]

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

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

Application Note from the ST author 5

The Firmware integrity and Correct TSF start-up tests are not done during normal operation of the TOE.

6.3.4.2 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) [*Clock invalid*

(4) Replace battery

(5) RAM error

(6) NV memory error

(7) measurement system error

(8) Fraud attempt][79]

6.3.4.3 Tamper notification (FPT_TNN.1)

FPT_TNN.1	*Tamper notification*

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

[78] [assignment: *list of self-tests run by the TSF,* [*assignment: list of additional self-tests run by the TSF on start-up*]]

[79] [assignment: *list of types of failures in the TSF,* [*assignment: list of other types of failures and recovery actions in the TSF*]]

Dependencies: None

FPT_TNN.1.1 The TSF shall monitor [*meter cover, terminal cover, metrology function*][80] and notify [the HES via the Communication Module][81] when physical tampering of the following types has occurred:

(1) Magnetic interference

(2) [*Terminal cover removal*

(3) Meter cover removal

(4) module cover removal

(5) Association authentication failure

(6) Decryption or authentication failure

(7) *Replay attack*][82]

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.

6.3.4.4 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***[83]: [m*etrologically certified data, credentials, meter configuration*][84].

[80] [assignment: *list of TSF devices/elements for which active detection is required*]
[81] [assignment: *designated user(s), role(s), or interface(s)*]
[82] [assignment: *list of additional physical tampering scenarios*]
[83] Refinement of "entities" consistent with section J.8 of [CC_P2].
[84] [assignment: *list of identified entities*]

FPT_RPL.1.2 The TSF shall ~~***perform***~~ [discard the message and [*record event log*][85] 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 [*reader, management, technician, upgrade*][86] the ability to query [the currently executing version of the TOE **firmware**[87]][88].

FPT_TSU.1.2 The TSF shall provide means to authenticate and verify the integrity of **firmware**[87] updates to the TOE prior to installing those updates, using a digital signature mechanism that meets the following: [*AES-GCM-128*][89].

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: [*encrypted and authenticated*][90].

FPT_TSU.1.4 The TSF shall provide [*upgrade*][91] the ability to activate updates to TOE **firmware**[87].

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.

---

[85] [assignment: *list of specific actions*]
[86] [assignment: *list of authorised roles*]
[87] *software/firmware* – cf. the Glossary definition of firmware applicable in this Protection Profile
[88] [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]
[89] [assignment: *mechanism specification*]
[90] [assignment: *list of additional properties*]
[91] [assignment: *list of authorised roles*]

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

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

Activation in FPT_TSU.1.4 results in the updated firmware being executed.

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

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

6.3.5 Security Management

6.3.5.1 Security roles (FMT_SMR.1)

FMT_SMR.1	*Security roles*

Dependencies: FIA_UID.1 Timing of identification[92].

FMT_SMR.1.1 The TSF shall maintain the roles [*management, technician, reader, pre-established, public, upgrade*][93].

FMT_SMR.1.2 The TSF shall be able to associate ***received messages and keys***[94] 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 or maintenance roles.

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

6.3.5.2 Management of Security Functions Behaviour (FMT_MOF.1)

FMT_MOF.1	*Management of Security Functions Behaviour*

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

[93] [assignment: *the authorised identified roles*]

[94] 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.

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*[95] the functions listed in the *TSF Configuration Table*[96] to the authorised identified roles in the *TSF Configuration Table*[97].

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 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 16 - TSF Configuration Table

ID	Function	Configurable status	Roles Authorised for Configuration
(i)	Allowed number of consecutive failed authentication attempts (FIA_AFL.1)	[*Configurable*][98]	[*management, technician*][99]
(ii)	Time period for blocking access after the allowed number of consecutive failed authentication attempts has been exceeded (FIA_AFL.1)	[Configurable][100]	[*management, technician*][101]
(iii)	Protection level applied to exchange of categories of application data (FDP_IFF.1/Msgs)	[Not configurable][102]	[*None*][103]
(iv)	Triggering of an alarm on the occurrence of an event (FAU_ARP.2)	[Configurable][104]	[*management, technician*][105]
(v)	Destination of an alarm on the occurrence of an event (FAU_ARP.2)	[Configurable][106]	[*management, technician*][107]

[95] [selection: determine the behaviour of, disable, enable, modify the behaviour of]
[96] [assignment: *list of functions*]
[97] [assignment: *the authorised identified roles*]
[98] [selection, choose one of: Configurable, Not configurable]
[99] [assignment: *the authorised identified roles*]
[100] [selection, choose one of: Configurable, Not configurable]
[101] [assignment: *the authorised identified roles*]
[102] [selection, choose one of: Configurable, Not configurable]
[103] [assignment: *the authorised identified roles*]
[104] [selection, choose one of: Configurable, Not configurable]
[105] [assignment: *the authorised identified roles*]
[106] [selection, choose one of: Configurable, Not configurable]
[107] [assignment: *the authorised identified roles*]

(vi)	Permissions allocated to roles (FDP_ACF.1, FDP_IFF.1/Msgs, FDP_IFF.1/Keys, FPT_TSU.1, FMT_MOF.1, FMT_MTD.1/Audit FMT_MTD.1/Time)	[Not configurable][108]	[*None*][109]

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 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*[110] the *audit log records*[111] to [management][112].

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*

[108] [selection, choose one of: Configurable, Not configurable]
[109] [assignment: *the authorised identified roles*]
[110] [selection: change_default, query, modify, delete, clear, [assignment: *other operations*]]
[111] [assignment: *list of TSF data*]
[112] [assignment: *the authorised identified roles*]

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*[113] the *meter time*[114] to [management*, technician, pre-established*][115].

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:* [*RAM error, NV memory error, measurement system error, Program memory error and Watchdog error*][116]
- *Physical tampering events:* [*Magnetic interference, Terminal cover removal, Meter cover removal*][117]
- *Other events:* [*clock invalid, replace battery*][118]

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: [Alarm push type and time][119]

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*[120].

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 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.

---

[113] [selection: change_default, query, modify, delete, clear, [assignment: *other operations*]]
[114] [assignment: *list of TSF data*]
[115] [assignment: *the authorised identified roles*]
[116] [assignment: *list of events and destination for the alarm for each event*]
[117] [assignment: *list of events and destination for the alarm for each event*]
[118] [assignment: *list of events and destination for the alarm for each event*]
[119] [assignment: *list of alarm messages and associated additional information*]
[120] [assignment: *rules that specify when an alarm must be sent relative to the detection of the event*]

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;***~~[121]

~~***b) All auditable events for the not specified***[122] ~~***level of audit;***~~ [123]~~***and***~~

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)

---

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

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

[123] 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.

u) Change of access rights (FAU_SAR.2, FMT_MOF.1)

v) Device error events as follows: [NV memory error, measurement system error]124 (FPT_BST.1, FPT_FLS.1)

w) Failure of the random bit generator ((FPT_BST.1, FCS_RNG.1)

x) Clearing the audit log (FAU_STG.1)

y) Security anomaly events as follows: [

(1) Magnetic interference,

(2) Terminal cover removal,

(3) Meter cover removal,

(4) Module cover removal,

(5) Association authentication failure,

(6) Decryption or authentication failure] [125]

z) Modification of [None]126

aa) Self-test completed [FPT_BST.1]

bb) [None]127.

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*][128].

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).

[124] [assignment: *list of auditable device error events*]
[125] [assignment: *list of auditable security anomaly events*]
[126] [assignment: *list of specified auditable data categories*]
[127] [assignment: *other specifically defined auditable events*]
[128] [assignment: *other audit relevant information*]

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 6

The meter can support the events as follow relate to [Load limitation configuration/activation]:

- Limiter threshold changed: Indicates that the limiter threshold has been changed
- Normal threshold changed: Indicates that the meter normal threshold value changed
- Emergency threshold changed: Indicates that the meter emergency threshold value changed

The event Magnetic interference can be found as Strong DC field detected in the Fraud event log. The customer doesn't need the Module cover removal, because there is a seal in the module cover. There is Module pull out event in the standard event channel.

For the [Failure of the random bit generator] of this event, the random number in the meter is 100% generated by the chip and will not fail, so there is no such event[Failure of the random bit generator].

For the [Self-test completed] event, if there is an error in the meter self-test, an event will be generated immediately. If no error event is generated, the meter will be considered to be in normal operation. So, there's no need for this event, because this event will happen every day.

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 [management, *technician, reader*][129] with the capability to read *the contents*[130] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in **the format specific in the following reference: [*[SX601][SX631]*]**[131].

[129] [assignment: *authorised users*]
[130] [assignment: *list of audit information*]

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

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 [DLMS/COSEM object model]***[132].

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*[133] ***~~unauthorised~~***[134] modifications to the stored audit records in the audit trail.

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

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*[135] if the audit trail exceeds: [*the maximum capacity, details in section 7.2*] [136]

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

---

[131] 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]*

[132] 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*]

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

[134] 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.

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

[136] [assignment: *pre-defined limit **in terms of number of records supported***]

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 17 - 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
	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

Assurance Requirements		
	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 18.

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[137]:
   - Authentication of message origin
   - Protection against replay of messages
   - Encryption of sensitive data
   - Integrity protection of message content
   - Authorisation rules to recognise sources that are permitted to send the message type.

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

   The Functional Specification shall identify any secure channels (or other secure communication mechanism) used for the import of secret or private keys or random bits (cf. Application Note 10, Application Note 19). The evaluator shall check that

[137] 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.

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 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 13 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 18 - 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.4		X	X						
FCS_COP.1/GUE		X		X			X		
FCS_COP.1/GBE		X		X			X		
FCS_COP.1/KE		X		X			X		
FCS_COP.1/Auth		X		X			X		
FCS_COP.1/FW		X		X			X		
FCS_RNG.1				X					
FDP_ACC.2	X		X						
FDP_ACF.1	X		X						
FDP_IFC.1/Msgs	X	X							
FDP_IFF.1/Msgs	X	X							
FDP_IFC.2/Int					X				
FDP_IFF.1/Int					X				
FDP_IFC.1/Keys	X			X					
FDP_IFF.1/Keys	X			X					
FDP_RIP.1			X						
FIA_UAU.6	X								
FIA_AFL.1	X								
FPT_BST.1						X			
FPT_FLS.1						X			
FPT_TNN.1								X	X
FPT_RPL.1		X							
FPT_STM.1								X	X
FPT_TSU.1							X		
FMT_SMR.1	X							X	X
FMT_MOF.1	X								X

	O.Authorisation	O.Messages	O.DataAtRest	O.Crypto	O.Interfaces	O.Resilience	O.SecureUpdate	O.Logging	O.Alarms
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 of [SM-MSR].

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 19 - Summary of Security Functional Requirements Dependencies

Requirement	Dependencies	Fulfilled by
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1 (for internally generated keys) See also note below on destruction of keys imported to the meter.
FCS_COP.1	[FDP_ITC.1 or	FCS_CKM.1 (for internally

Requirement	Dependencies	Fulfilled by
	FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	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.

Requirement	Dependencies	Fulfilled by
FDP_RIP.1	No dependencies	
FIA_UAU.6	No dependencies	
FIA_AFL.1	FIA_UAU.1	For this TOE the authentication conditions (and timing of authentication) for access to private data via the user interface are defined in FIA_UAU.6 (and the transitive dependency from FIA_UAU.1 to FIA_UID.1 is not applicable because users at the user interface are not individually identified).
FPT_BST.1	No dependencies	(Note that the completion of self-test is not required to be logged in this Protection Profile, but start-up and reset events and failures detected by the self-test are required to be logged – see FAU_GEN.1).
FPT_FLS.1	No dependencies	
FPT_TNN.1	No dependencies	
FPT_RPL.1	No dependencies	
FPT_STM.1	No dependencies	
FPT_TSU.1	FCS_COP.1	FCS_COP.1 Application Note 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

Requirement	Dependencies	Fulfilled by
		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 20 - 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	Depends On:	Which is:
		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
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

Component	Depends On:	Which 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

Metrology functions that are under legal metrological control are not part of the evaluation, including:

- Energy
- TOU
- Load Profile
- Relay
- Load Management-Relay control
- Demand
- Display
- Instantaneous Measurement
- Billing
- Identification numbers

Functions in the logical scope of the evaluation

- Clock and Calendar
- Event Record
- Errors and Alarms
- Security
- Push
- Firmware upgrade

Meter communication functions, including network interfaces and direct interfaces

- Optical Port
- RS485
- Communication Module
    - GPRS/4G module

- LTE-M module
- P1 Port

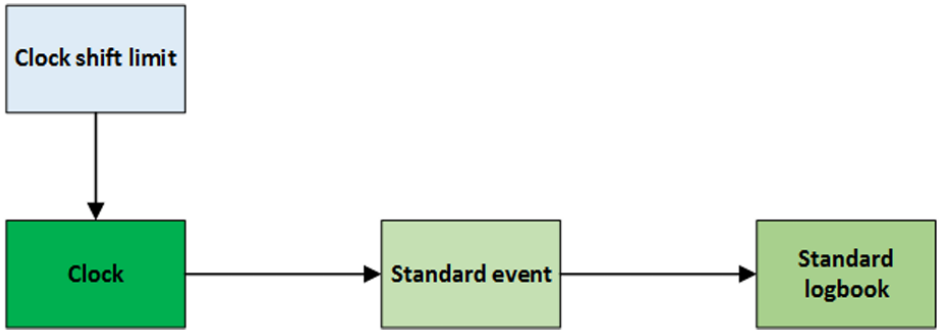
7.1 Clock and Calendar (SFR enforcing)

This IC models the device clock, managing all information related to date and time including deviations of the local time to a generalized time reference (UTC) due to time zones and daylight-saving time schemes. The IC also offers various methods to adjust the clock.

The date information includes the elements year, month, day of month and day of week. The time information includes the elements hour, minutes, seconds, hundredths of seconds, and the deviation of the local time from UTC.

Meter support to be synchronized the date and time by PC software locally and the ARM system remotely through DCU and Gateway.

Figure 18 - Clock management process



When the synchronization is out of the clock_shift_limit, meter will generate a log in the standard event. And the range of clock_shift_limit can be changeable (default: 180 seconds).

Configuration for the meter time is available only for management, technician and pre-established roles.

Clock errors occur in extreme cases, e.g., after meter power up, the RTC is not Accurate due to the disconnect or discharge of energy storage device. In this case, meter will have corresponding operation to solve errors.

1. Alarm LED light will open until meter receives new time setting data.
2. Bit0 (critical error) or Bit1 (clock invalid) of AMR profile status will be set and save in the load profile.

Enforced SFRs: FPT_FLS.1 (Clock invalid), FPT_STM.1, FMT_MTD.1/Time

7.2 Event Record (SFR enforcing)

Events are generated by the meter itself or by its environment. All these events are logged in several event logs. Every event has a unique code to identify the action which has triggered it. Every event (except Event log cleared) is assigned to one event log and it is only stored there.

Instances of event code objects are captured in corresponding event logs. Event log objects are instances of COSEM class "profile generic" and are used to store events. They are organized as FIFO buffers where records are sorted by time. Once the buffer is full, the oldest entry in the buffer is the first to be replaced. The capacity (maximum number of records in a buffer) of the event log objects varies from object to object, detail reference the next table Event log objects. Records in the buffer are captured asynchronously, as the events occur.

The majority of the supported event log objects (except for Power failure event log) follow the same basic structure containing the time stamp (time of the occurrence of the event) and the event code object.

The event logs and audit records are readable for users with management, technician and reader roles. Deletion of the audit log records is available only for management and technician roles. These access rights are covered by the DLMS/Cosem object model [OBIS_LIST].

The meter features the following event log objects:

Table 21 - Event log objects

Event log object	Logical Name	Capacity
Standard event log	0-0:99.98.0.255	100
Fraud detection log	0-0:99.98.1.255	30
Disconnector control log	0-0:99.98.2.255	10
Power quality event log	0-0:99.98.4.255	100
Communication event log	0-0:99.98.5.255	100
Phase interruption log	1-0:99.97.1.255	100
Output Control K1 log	0-0:99.98.20.255	10
Image activate log	0-0:99.98.22.255	10
Security event log	0-0:99.98.26.255	100
Power failure event log	1-0:99.97.0.255	100

Special case:

- FAU_GEN.1.1 u) Change of access rights
    - The access rights cannot be changed during normal operation. It is only possible with a new firmware.

Enforced SFR: FMT_MTD.1/Audit, FAU_GEN.1, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.3.

Support SFRs: FAU_ARP.2.

7.2.1 Standard event log

Standard event log contains all events not recorded in a special event log. Standard event log structure consists of timestamp and event code. Standard event log code object holds the code from the last event triggered. These codes along with timestamps are then used in event log.

Table 22 - Standard event list

Event Code	Event Name	Event 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 lifetime.
8	Battery voltage low	Indicates that the current battery voltage is low.
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 that the meter program memory error
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 nonvolatile 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.
19	Passive TOU programmed	Indicates signal detected on the meter's input terminal.
20	External alert detected	Indicates a external alert detected
47	One or more parameters changed	Indicates one or more parameters have been modified
48	Global key(s) changed	One or more global keys changed.
51	FW verification failed	Indicates the transferred firmware verification failed i.e. cannot be activated.
52	Unexpected consumption	Indicates consumption is detected at least on one phase when the disconnector has been disconnected.

89	Missing neutral	Indicates that the neutral connection from the supplier to the meter is interrupted (but the neutral connection to the load prevails). The phase voltages measured by the meter may differ from their nominal values.
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.
258	External pin reset	Indicates abnormal reset of the meter due to the reset pin of the MCU during the operation of the meter
259	Power up/down reset	Indicates meter reset due to system power supply during meter operation
261	4G module FW upgrade successful	Indicates the module upgrade successful
262	Flash Memory error	Indicates the meter flash memory error
267	Clear all	Indicates energy, event information, load curve, event log and other events are cleared to 0
292	Module insertion	Indicates that the module is inserted into the meter
293	Module pull out	Indicates that the module is removed from the meter

7.2.2 Fraud event log

Fraud event log contains all events related to the detection of fraud attempts.

Table 23 - Fraud event list

Event code	Event name	Event description
40	Terminal cover removed	Indicates that the terminal cover has been removed.
41	Terminal cover closed	Indicates that the terminal cover has been closed.
42	Strong DC field detected	Indicates that a strong magnetic DC field has been detected.
43	No strong DC field anymore	Indicates that the strong magnetic DC field has disappeared.
44	Meter cover removed	Indicates that the meter cover has been removed.
45	Meter cover closed	Indicates that the meter cover has been closed.
46	Association authentication failure (5-time failed authentication)	Indicates that a user tried to gain LLS access with wrong password (intrusion detection) access challenge processing failed n-times
48	Global key(s) changed	One or more global keys changed
49	Decryption or authentication failure (5-time failure)	Indicates that a user tried to gain HLS access with wrong key (intrusion detection) access challenge processing failed n-times
50	Replay attack	Receive frame counter value less or equal to the last successfully received frame counter in the received APDU Event signalizes the situation as well when the DC has lost the frame counter synchronization.
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.
518	Current reversal L1	Indicates the reverse power is greater than 20w and the switching duration is greater than 30s
519	Current reversal L2	Indicates the reverse power is greater than 20w and the switching duration is greater than 30s;only for three phase meter
520	Current reversal L3	Indicates the reverse power is greater than 20w and the switching duration is greater than 30s;only for three phase meter
521	Current eversal L1 end	Indicates reverse power is not greater than 20w, no end delay threshold judgment
522	Current eversal L2 end	Indicates reverse power is not greater than 20w, no end delay threshold judgment; only for three phase meter
523	Current eversal L3 end	Indicates reverse power is not greater than 20w, no end delay threshold judgment; only for three phase meter
528	Current eversal end	Reverse power is not greater than 20w, no end delay threshold judgment

7.2.3 Disconnector control log

Table 24 - Disconnector control event list

Event code	Event name	Event 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
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.
285	Unexpected consumption end	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.
790	Normal threshold changed	Indicates that the meter normal threshold value changed
792	Emergency threshold changed	Indicates that the meter emergency threshold value changed

7.2.4 Power quality event log

Table 25 - Power quality event list

Event code	Event name	Event description
76	Under voltage L1	Indicates under voltage on at least L1 phase was detected.
77	Under voltage L2	Indicates under voltage on at least L2 phase was detected.
78	Under voltage L3	Indicates under voltage on at least L3 phase was detected.
79	Overvoltage Ll	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 Ll	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 Ll normal	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
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.
286	Phase sequence reversal end	Recover from reverse phase sequence state to non-reverse phase sequence state; Only for three phase meter
1024	Phase Asymmetry End	The maximum current is less than 0.05Ib or (Imax-Imin) < unbalance value, and there is no end delay threshold judgment;only for three phase meter
1025	Reverse polarity start	The phase line and neutral line are swapped, and the phase voltage is greater than 0.5Un and the duration is greater than 30s. only for three phase meter
1026	Reverse polarity end	Indicates the reverse polarity event end;only for three phase meter
1033	Overcurrent Started Phase L1	Indicates overcurrent on at least L1 phase was detected.
1034	Overcurrent Started Phase L2	Indicates overcurrent on at least L1 phase was stopped.
1035	Overcurrent Started Phase L3	Indicates overcurrent on at least L2 phase was detected.
1036	Overcurrent Ended Phase L1	Indicates overcurrent on at least L2 phase was stopped.

1037	Overcurrent Ended Phase L2	Indicates overcurrent on at least L3 phase was detected.
1038	Overcurrent Ended	Indicates overcurrent on at least L3 phase was stopped.
1039	Missing current	In a three-phase meter, one or two phases have a current less than 0.4%Ib, and the corresponding phase voltage is greater than 50%Un, and at least one phase current is greater than 5%Ib, and the duration is greater than 60s. In a single-phase meter, the current is less than 0.4%Ib, and the phase voltage is greater than 50%Un and the duration is greater than 60s.
1040	Missing current end	Indicates the missing current end
1041	Voltage Imbalance Condition	Indicates that the meter "Maximum voltage per second" difference between minimum voltage greater than 50% Maximum voltage
1042	Voltage Imbalance Cleared	Indicates that the meter "Maximum voltage per second" difference between minimum voltage less than 50% Maximum voltage
1047	Over current in any phase	At least one phase current exceeds the set value, and the duration exceeds the set value
1048	Over current in any phase end	The current of each phase is less than the set value and the duration is greater than the set value

7.2.5 Communication event log

Table 26 - Communication event list

Event code	Event name	Event description
140	No connection timeout	There has been no remote communication on application layer for a predefined period of time, i.e. meter could not be reached remotely.
141	Modem Initialization failure	Indication that there was an incorrect modem response to the AT initialization command or that no response was received
142	SIM Card failure	SIM card is not inserted or is not recognized
143	SIM Card ok	SIM card has been correctly detected
146	PDP context established	PDP context is established
147	PDP context destroyed	PDP context is destroyed
148	PDP context failure	Indication that returns PDP content is not valid
149	Modem SW reset	Modem restarted by SW reset
150	Modem HW reset	Modem restarted by HW reset (this event is not issued after a general power resume)
151	GSM outgoing connection	Modem is successfully connected, initiated by an outgoing call.
152	GSM incoming connection	Modem is successfully connected, initiated by an incoming call
153	GSM hang-up	Modem is disconnected
154	Diagnostic failure	Indication that the modem response to diagnostic AT commands is incorrect, wrong, or that no response has been received
155	User initialization failure	Indication that the initialization AT modem command is wrong, after an error message or without a modem response
156	Signal quality low	Signal strength too low, not known, or not detectable

157	Auto Answer Number of calls exceeded	Number of calls has exceeded (in mode(1) or mode(2)) the values given in the attribute number_of_calls.
158	Local communication attempt	Indicates a successful communication on any local port has been initiated
1280	Unexpected ADPU	AARQ Error
1281	Unauthorized access	Indicates access with the Obis object does not exist or the attribute does not exist, or the permission is incorrect

7.2.6 Output Control K1 log

Table 27 - Output Control K1 log

Event code	Event name	Event description
3584	Auxiliaryrelay1 remote connection	Indicates that the auxiliaryrelay1 has been remotely connected
3585	Auxiliaryrelay1 remote disconnection	Indicates that the auxiliaryrelay1 has been remotely disconnected
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.

7.2.7 Security event log

Table 28 - Security event list

Event code	Event name	Event description
46	Association authentication failure (n time failed authentication)	Indicates that a user tried to gain LLS access with wrong password (intrusion detection) access challenge processing failed n-times
49	Decryption or authentication failure (n times failure)	Indicates that a user tried to gain HLS access with wrong key (intrusion detection) access challenge processing failed n-times
255	Deleted security events	Indication that the book of events relating to meter safety has been deleted
531	Authentication successful	Indicates that success password(LLS) or key(HLS) communication when a link is successfully established every time
1281	Unauthorized Access	Indicates access with the Obis object does not exist or the attribute does not exist, or the permission is incorrect
3073	Change cryptographic keys or credentials failed	Indicates change the keys (LLS,HLS) or HLS setting(include policy) failed
3074	Message authentication failed	it means the message signature verify wrong

7.2.8 Phase interruption log

Table 29 – Phase interrupt log

Event code	Event name	Event description
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. Only for three phase meter
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. Only for three

		phase meter
85	Voltage L1 normal	Indicates that the mains voltage is in normal limits again, e.g. after overvoltage.
87	Voltage L2 normal	Indicates that the mains voltage is in normal limits again, e.g. after overvoltage. Only for three phase meter
87	Voltage L3 normal	Indicates that the mains voltage is in normal limits again, e.g. after overvoltage. Only for three phase meter
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.

7.2.9 Image activate log

Table 30 – Image activate log

Event code	Event name	Event description
18	Firmware activated	The meter's new firmware was successfully migrated and verified
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.

7.2.10 Power failure event log

Power failure event log contains all events related to long power outages, i.e., start of a long power outage.

It is a simplified version of the full power quality event log storing just the timestamp and the duration of last long power failure in any phase. The timestamp represents the start of power failure. The object Duration of last long power failure in all three phase (0-0:96.7.15.255) stores only the duration of the most recent power outage.

Time thresholds for long power failure are defined with Time threshold for long power failure object (0- 0:96.7.20.255).

7.3 Errors and Alarms (SFR enforcing)

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.

The alarm message is defined in Data-Notification format，as follows：

Data-Notification ::= SEQUENCE

{

long-invoke-id-and-priority,

date-time ,

notification-body

}

long-invoke-id-and-priority: Alarm push type（According to IDIS definition, value is 00 00 00 04）

date-time: Alarm push time

notification-body：The specific information of the push object， it can be set in PUSH setup, and the meter can be configured as event logs. If configured as event logs, the push message will include the time and code of the event occurrence.

If the remote communication channel is idle and the module is already connected, the meter will immediately send. If these two conditions are not met, the meter will wait until both conditions are met before sending

Enforced SFR: FAU_ARP.2.

7.3.1 Alarm register

Each bit in the alarm registers represents a different alarm. If the bit is set 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.

Table 31 - Alarm 1 register

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

Note: the definition of error register is same to alarm1 register.

Table 32 - Alarm 2 register

Bit	**Alarm**	Triggering event
0	Total Power Failure	1
1	Power Resume	2
2	Voltage Missing Phase Ll	82
3	Voltage Missing Phase L2	83
4	Voltage Missing Phase L3	84
5	Voltage Normal Phase Ll	85
6	Voltage Normal Phase L2	86
7	Voltage Normal Phase L3	87
9	Phase Asymmetry	90
10	Current Reversal	91
11	Wrong Phase Sequence	88
12	Unexpected Consumption	52
13	Key Exchanged	48
18	Local communication attempt	158
31	Disconnect/Reconnect failure	68

7.3.2 Alarm filter

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.

7.3.3 Alarm descriptor

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 HES.

7.4 Security (SFR enforcing)

E-meter security is devised into Physical Security and Logical Security.

7.4.1 Physical Security

The terminals of the consumption meter are located under the terminal cover. The fixing screws of the terminal cover can be sealed by the power supplier, which prevent unauthorized access to the phase connections. There are three switches to detect if terminal cover, meter cover or front cover were opened or closed. The LCD indicator as specified according to chapter "5.3.1 LCD" of [SX601] and/or [SX631]. It also can be saw the time of event triggered in fraud event log. If there is an external magnetic field near the meter, the event of Strong DC field detected will be triggered. These functions support the prevention of tampering with the measurement and the security of the data contained therein.

Enforced SFRs: FPT_TNN.1

7.4.2 Logical Security

E-meter supports six different clients with three different behaviours regarding authentication minimal requirements, as shown in following table:

Table 33 - Different clients with three different behaviours

Client name	Client L-SAP	Minimal Security Requirements
Public	16	Lowest level security (no security)
Reader	32	HLS or LLS
Technician	48	HLS or LLS
Management	1	HLS or LLS
Pre-established	102	No HLS nor LLS
Upgrade	64	HLS or LLS

7.4.2.1 Data access security

Data access security is managed by the Association LN object. Each COSEM server i.e., a logical device may support Application Associations with various clients, each having a different role, and with this different access rights. Each Association object provides a list of objects visible in that Application Association and the access rights to objects' attributes and methods. To be able to access data, the client must be properly authenticated. Upon Application Association establishment, an authentication context is negotiated between the client and the server. This specifies the required authentication of the peers, and, where needed, the security algorithm to verify the authentication. Two data access security levels are provided:

- Lowest level security (no security).
- Low Level Security (LLS).
- High Level Security (HLS).

The roles and access rights are defined in the DLMS/Cosem object model [OBIS_LIST]. For details, please see [AGD] section 2.3 User Roles.

Enforced SFRs: FDP_ACC.2, FDP_ACF.1, FDP_IFC.1/Msgs, FDP_IFF.1/Msgs, FMT_SMR.1, FMT_MOF.1[138].

7.4.2.2 Data transport security

Data transport security relies on applying cryptographic protection to xDLMS APDUs. This is achieved via several security mechanisms. The first mechanism is incorporated in application association request with the COSEM application context, The table below shows different application context names and the relation between those names and allowed types of xDLMS APDUs. Ciphered APDUs are allowed only in Application context name with ciphering.

Table 34 - Different application context names

Application ContextName	ID	Unciphered APDUs	Ciphered APDUs
Logical Name Referencing no ciphering	0	Yes	No
Logical Name Referencing with ciphering	3	Yes	Yes

Enforced SFRs: FDP_IFC.1/Msgs, FDP_IFF.1/Msgs.

7.4.2.3 Replay protection

The meter records a frame counter value for each client in the meter. The factory initial value is 0.

When the meter receives the frame counter value in the data frame sent by the client is less than or equal to the frame counter value recorded in the meter, the meter will refuse communication and record corresponding events.

When the meter receives the frame counter value in the data frame sent by the client is greater than the frame counter value recorded in the meter, the meter will allow the communication.

After successful communication, the FC[139] value recorded in the meter will be updated to the frame counter value of successful communication

The meter can clear this frame counter value by modifying the key. If the frame counter value reaches 0xffffffff value, it cannot communicate, so it is necessary to modify the key regularly

Enforced SFRs: FDP_IFF.1/Msgs., FPT_TNN.1 (Replay attack), FPT_RPL.1

7.4.2.4 Security suite

A security suite determines the cryptographic algorithm used for message security. A security suite is identified with a Security Suite ID. Security suite (0) utilizes the Galois/Counter Mode (GCM) with AES-128. In this security suite, global keys are protected during transportation using the AES-128 key wrap algorithm.

[138] Every configuration parameter (DLMS/Cosem object) can be found in [OBIS_LIST]. This object model cannot be changed only via a FW upgrade. A parameter can be changed if there is a role with SET, or ACTION right configured.
[139] Frame Counter

Enforced SFR: FCS_COP.1/KE.

Table 35 - Security suite

Security Suite id	Authenticated encryption	Digital signature	Hash	Key transport
0	AES-GCM-128	N/A	N/A	AES-128 Key wrap
1	AES-GCM-128	ECDSA with P-256	SHA 256	AES-128 Key wrap
2	AES-GCM-256	ECDSA with P-384	SHA 384	AES-256 Key wrap

The key generation is done in the factory, and the unique per device keys are preloaded to the meters before delivery. When a new set of keys are loaded to the device the previous keys are overwritten.

Enforced SFRs: FCS_CKM.4, FDP_IFF.1/Msgs, FDP_RIP.1.

7.4.2.5 Security policy

Enforces authentication and/or encryption using the security algorithms available within the security suite. It applies independently for requests and responses. The following security policies are specified and allowed:

- (0) nothing,
- (1) all messages to be authenticated,
- (2) all messages to be encrypted,
- (3) all messages to be authenticated and encrypted
- (4)…(15) reserved

The TOE uses Security Policy 3, which means that every message is authenticated and encrypted using the proper keys.

The access rights may require stronger protection than what is required by the security policy.

Since every message is authenticated and encrypted there is no need for re-authentication.

The meter will periodically check the integrity of these key data. Once an error is found, the meter will be restored based on the backup data.

Enforced SFRs: FCS_COP.1/GUE, FCS_COP.1/GBE, FCS_COP.1/Auth, FDP_IFC.1/Msgs, FDP_IFF.1/Msgs, FIA_UAU.6.

By the default configuration of the TOE after 5 failed authentication the TOE blocks access for that entity via the relevant interface to data requiring prior authentication until the configured time, in this case 1 minute. These values can be configured by a user with management or technician roles.

Enforced SFRs: FIA_AFL.1, FPT_TNN.1 (Association authentication failure, Decryption or authentication failure).

7.4.2.6 Secure storage

Secure storage is a reserved space in EEPROM which is cryptographically protected. In secure storage E-meter stores all the necessary global encryption, authentication, and master keys.

Table 36 - Keys

Key	Description
Master key (MK)	A cryptographic key that is used for the encryption or decryption of other keys (key encryption key)
Global Unicast Encryption Key (GUEK)	The key for AES-GCM-128 when the security control word bit 6 = 0 unicast.
Global Broadcast Encryption Key (GBEK)	The key for AES-GCM-128 when the security control word bit 6 = 1 broadcast.
Authentication Key (AK)	Additional information for AES-GCM-128 when protect method is authenticate only or authenticate and encryption.

Keys can be changed using the correct encryption algorithm, RFC 3394 AES Key Wrap, and the TOE related MK for as the encryption key. If the keys are coming from an unauthorized source, which means the keys used for authentication and encryption are invalid the message, as all the other unauthorized messages, are rejected and dropped by the TOE without processing.

(1) The keys stored in the meter cannot be read in a plaintext format for two reasons, first the keys are not stored in plaintext format in any case or scenario, and second reading the keys directly is not implemented in the TOE.

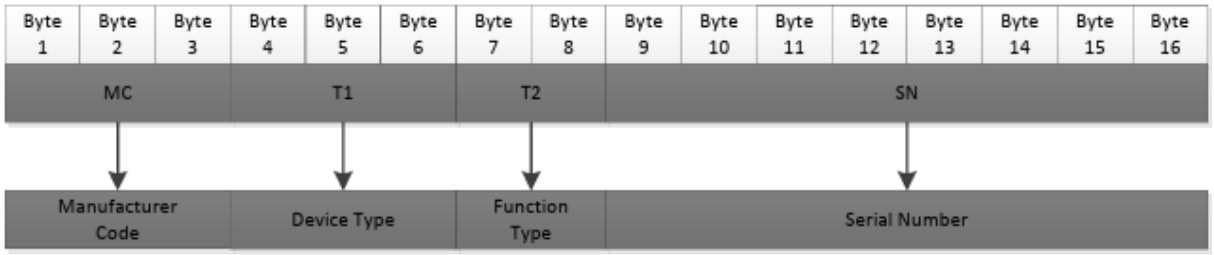
Even if the message is valid, and the keys are matching, if the received keys do not have the correct length the TOE will reject to replace the keys in use.

Enforced SFRs: FDP_IFC.1/Keys, FDP_IFF.1/Keys.

The COSEM logical device can be identified by its unique COSEM logical device name. This name can be retrieved from an instance of IC "SAP assignment", or from a COSEM object named "COSEM logical device name". The name is of type octet-string of up to 16 octets in size.

The following figure presents the division of the "COSEM logical device name" as enforced by the IDIS association:

Figure 19 - Definition of COSEM logical device name



The first three octets (MC) are ASCII encoded and uniquely identify the manufacturer of the device. The next three octets (T1) present ASCII encoded IDIS device type.

Table 37 - The T1 meaning

Device Type	Meaning
000 … 098	Reserved for non-IDIS meters; system title is considered as manufacturer specific

099	Reserved system title for the DC
100	IDIS package1 PLC single phase meter
101	IDIS package1 PLC poly phase meter
102	IDIS package2IP single phase meter
103	IDIS package2IP poly phase meter
104…255	Reserved for future use

The next two octets (T2) present ASCII encoded IDIS function type. The IDIS function types have the following meanings:

Table 38 - The T2 meaning

Function Type	Bit Meaning
Bit0 = 1	Disconnector extension
Bit1 = 1	Load Management extension
Bit2 = 1	Multi Utility extension
Bit3 = 1	Reserved for future use by IDIS

Last eight octets (SN) present ASCII encoded E-meter serial number as specified in COSEM object "Device ID" [0-0:96.1.0.255].

Example of the COSEM logical device name for SANXING three Phase Smart Meter with disconnector, multi-utility, and load management functionality with the Device ID 00000001:

Table 39 - logical device name for SANXING

MC			T1			T2		SN							
Byte1	Byte2	Byte3	Byte4	Byte5	Byte6	Byte7	Byte8	Byte9	Byte10	Byte11	Byte12	Byte13	Byte14	Byte15	Byte16
A	U	X	1	0	3	0	7	0	0	0	0	0	0	0	0

7.4.2.7 Random Number Generation

The random number of the meter uses the hard random number inside the chip. Please refer to the website for relevant instructions: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?validation=35435.

Based on the website above, the chip has 3 generation methodology, and will use the Simple Discard Method (A.5.1)

Enforced SFR: FCS_RNG.1.

7.4.3 Secure state preservation and self-tests

The TOE will preserve its secure state even with failures in the operation. The following events are identified in the TOE:

(1) Watchdog trigger results in meter reset:

When the meter powered on, will read system reset register form the MCU, if the WDT_RST bit of system reset register be set to 1, Watchdog trigger results in meter reset will record.

(2) Failure of the random bit generator:

When the meter receive correct AARQ for HLS5 association, will take the random number generator which provided by the MCU generator several string of Random bits if all the string is same, Failure of the random bit generator is record.

(3) Clock invalid: see section 7.1 of this document

(4) Replace battery:

The electricity meter detects the external battery voltage every second. When the tested battery voltage drops below 3.3V for 3 consecutive seconds, a replace battery event is recorded

(5) RAM error:

The meter checks the RAM data of different areas every second, such as soft clock, event threshold parameters, etc. The meter calculates the CRC of these data and compares it with their CRC in RAM. If any areas data is not equal, the RAM ERROR event is recorded.

(6) NV memory error:

The meter generates a 4-byte random data every minute, writes this random data to the designated area (a total of 128 bytes, 4 bytes written each time, loop writing), and then read the 4-byte data from designated area of EEPROM. If the generated random data is not equal to the read data, an NV error event is recorded.

(7) Measurement system error:

Each task cycle of the electricity meter reads a parameter from the metering chip and compares it with the metering parameters stored in the meter. If this is not equal for three times, the meter restarts the metering chip and reads the parameter again. If it is not consistent with the parameters stored in the meter, a metering error event is recorded

(8) Fraud attempt: see section 7.2.1 of this document.

The TOE runs a self-test during power on and normal operation. The tests are the following:

(1) Firmware integrity test:

When the meter powered on，the boot program calculates the CRC16 of the app firmware（Except the last 2 bytes），compares this CRC16 with the last 2 bytes of the firmware. If the verification is successful, runs part of the app program. If the comparison fails, repeat the calculation and comparison until the comparison is successful.

(2) Random bit generator test

When the meter receive correct AARQ for HLS5 association, will take the random number generator which provided by the MCU generator several string of Random bits if all the string is same, Failure of the random bit generator is record.

(3) Correct TSF start-up

When the meter start-up (power on) every time, it will perform the following security self-tests:

- RAM error,

- NV memory error,
- measurement system error,
- Meter configuration integrity test,
- Metrologically certified data integrity test,
- EE and flash device normal verification.

(4) [Meter configuration integrity test

For the sensitive data, such as certified data, key,

The meter will perform CRC16 verification, and the data will be encrypted through algorithm AES-ECB-128.

The meter will periodically check the integrity of these key data. Once an error is found, the meter will be restored based on the backup data.

(5) Metrologically certified data integrity test

The metrologically storage blocks are divided into three categories: primary RAM, backup RAM, and EEPROM, with the same storage structure.

Unit: 10Wh

Main area RAM: Retrieve more than 10Wh of electricity per second from the last count of electricity and store it in the main area.

Backup Area RAM: When there is a change in the RAM data of the primary and secondary areas, it is necessary to backup one copy to the backup area RAM.

EEPROM: Write the RAM data of the main area into EEPROM during power failure; When the RAM data in the main/backup area is abnormal, the number of recoveries from EEPROM

According to the main/backup area; When powered on, the remaining amount of electricity is stored in the integer energy EEPROM and then cleared in the EEPROM.

Storage structure: The storage structure is consistent with the last digit battery.

Note: The RAM in the main backup area is not initialized during reset. When the chip is powered on, the data in the main backup area will never be lost.

(6) EE and flash device normal verification

Every minute the meter will write 4Byte random number to the EE and flash, and then read it out, and compare it with the random number write to it. If failed, the NV memory error event will be record.

(7) RAM error:

The meter checks the RAM data of different areas during power-on or after reset, such as soft clock, event threshold parameters, etc. The meter calculates the CRC of

these data and compares it with their CRC in RAM. If any areas data is not equal, the RAM ERROR event is recorded.

(8) NV memory error:

The meter generates a 4-byte random data power-on or after reset, writes this random data to the designated area (a total of 128 bytes, 4 bytes written each time, loop writing), and then read the 4-byte data from designated area of EEPROM. If the generated random data is not equal to the read data, an NV error event is recorded.

Enforced SFRs: FPT_FLS.1, FPT_BST.1

7.4.4 Device ID (SFR non-interfering)

Meter has six different device ID's:

- Device ID 1 – E-meter serial number (e=0)
- Device ID 2 – E-meter equipment ID (e=1),
- Device ID 3 – function location (e=2)
- Device ID 4 – location information (e=3)
- Device ID 5 – no special meaning defined (e=4)
- Device ID 6 –IDIS certification number (e=5)

7.4.4.1 Device ID 1

Device ID1 is E-meter factory serial number (also reflected in a COSEM logical device name). The number is ASCII encoded. The length of the ID is between 4 and 16 octets.

7.4.4.2 Device ID 2

Device ID2 is customer ID. The number is ASCII encoded. The length of the ID must not exceed forty-eight (48) octets.

7.4.4.3 Device ID 3

Device ID3 represents function location. The number is ASCII encoded. The length of the ID must not exceed forty-eight (48) octets.

7.4.4.4 Device ID 4

Device ID4 includes location information. The number is ASCII encoded. The length of the ID must not exceed forty-eight (48) octets.

7.4.4.5 Device ID 5

Device ID5 has no special meaning defined. It is general purpose ID for any identification purposes. The number is ASCII encoded. The length of the ID must not exceed forty eight (48) octets.

7.4.4.6 Device ID 6

Device ID 6 is IDIS certification number. The number is ASCII encoded. The length of the ID must not exceed forty-eight (48) octets.

7.5 Push (SFR supporting)

The push messages are protected according to Security Policy 3, which means all messages are authenticated and encrypted.

DLMS messages can be "pushed" to a destination without explicit request. Push is initiated by a trigger, such as:

- Reach the scheduled time
- The value of local monitoring exceeds the threshold.
- Local events (such as power failure, power on, push button, meter cover opening, etc.)

PUSH data format is in accordance with Data-Notification. Push has the following functions:

- All Push objects can be set remotely and locally. The push object is no limit.
- All Push parameter (such as randomisation_start_interval, number_of_retries, repetition_delay) can be set separately through remote and local.
- The unfinished Push before power failure can be reported after power on again
- Interval 1, Interval 2, Interval 3, and Consumer Information support 4 groups of time and date.

7.5.1 Push Object type

There are 9 types of push for meters ,such as follow :

Table 40 - Push object types

Event code	Event name	Event description
1	Interval_ 1	0-1:25.9.0.255
2	Interval_2	O-2:25.9.0.255
3	Interval_3	0-3:25.9.0.255
4	Alarm	0-4:25.9.0.255
5	Installation	0-7:25.9.0.255
6	Power Down (Last gasp)	0-5:25.9.0.255
7	Warning message	O-8:25.9.0.255

Supported SFRs: FAU_ARP.2

7.6 Firmware upgrade (SFR enforcing)

E-Meter and Communication module upgrade features are as follows:

- Support broadcast upgrade and point-to-point upgrade.
- Support continuous upgrade after communication interruption.
- If some upgrade packages fail to be transmitted, supplementary transmission of these upgrade packages is supported.
- Support locally and remotely
- The meter action digital signature mechanism for FW integrity with the CRC and AES_GCM_128 tag

7.6.1 Transmission state diagram

Figure 20 - Transmission state diagram part 1

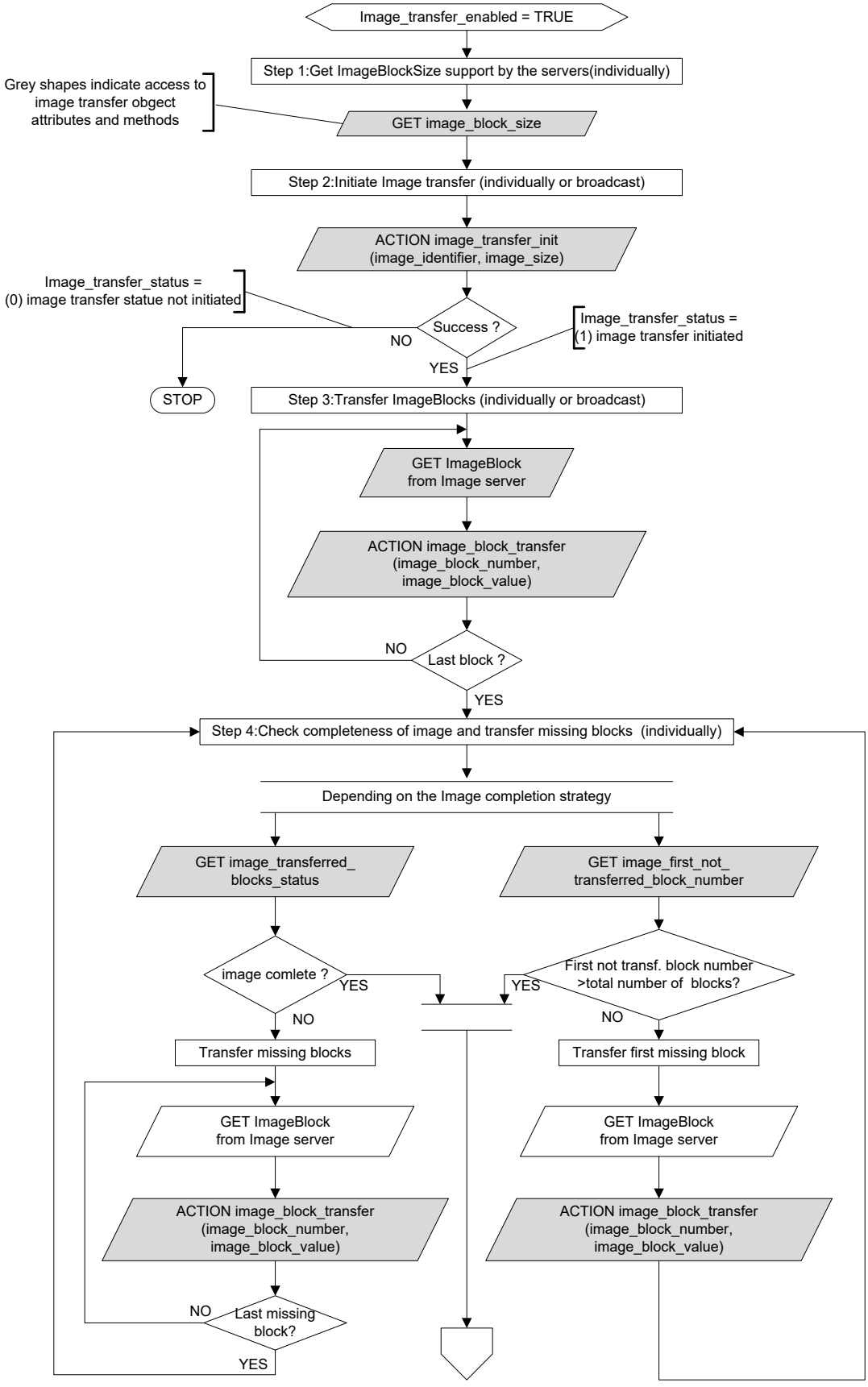
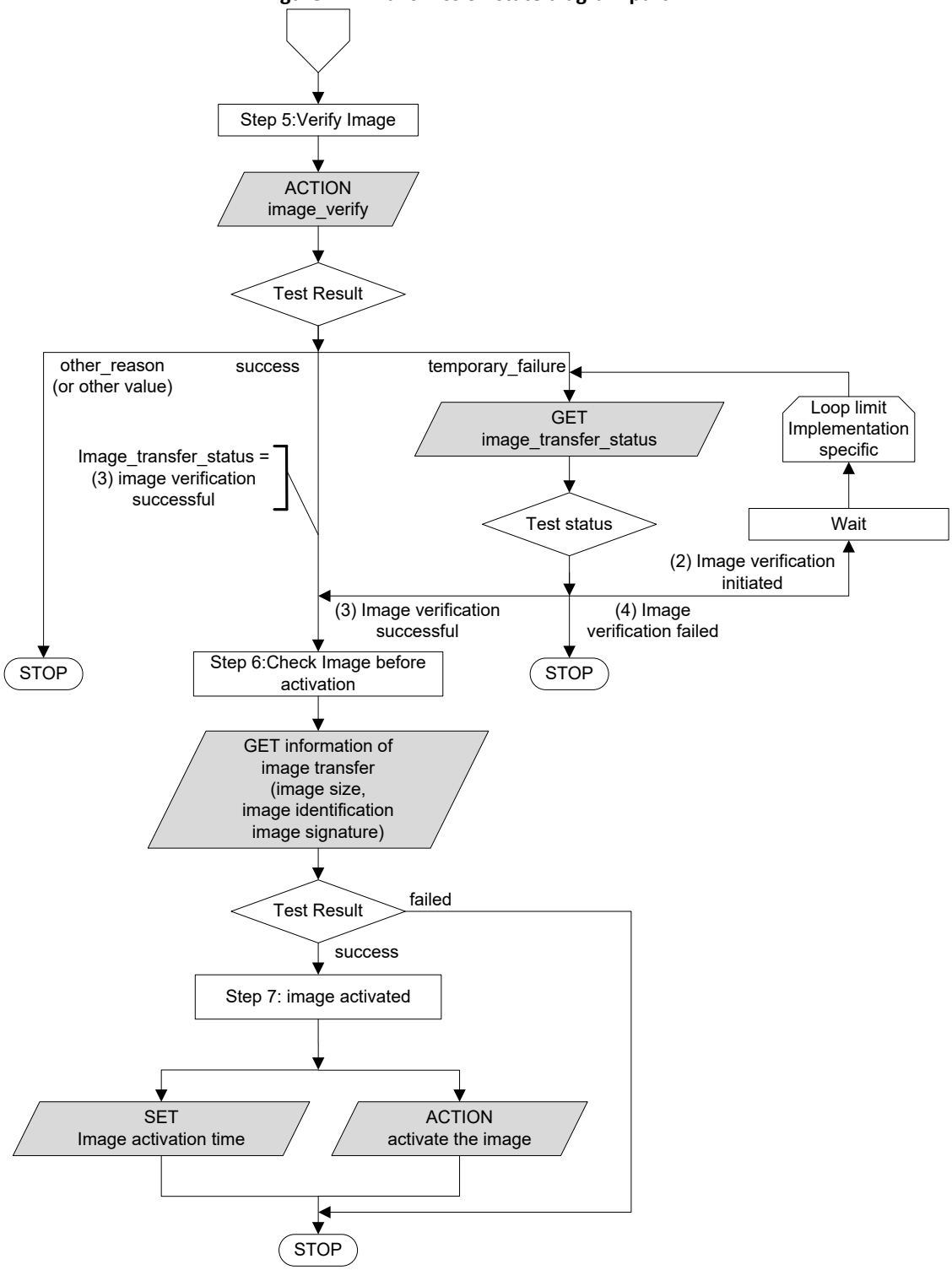


Figure 21 - Transmission state diagram part 2



7.6.2 Transmission state diagram

Prerequisite: mirror transfer needs to be turned on: image_transfer_enabled = TRUE.

Setting image_transfer_enabled to FALSE will disable all methods (calling these methods failed), and scheduled upgrade will also be disabled.

Status attribute is undefined (attribute reading is not restricted) 416 Q/SX J03.04.267-2022

Step 1 (optional): Get ImageBlockSize.

If the client doesn't know the size of the mirror block that the target server of mirror transfer can handle, before starting the process, the client should read the image_block_size attribute of the related "mirror transfer" object of each server that needs to transfer the mirror. The client can transmit the correct ImageBlocks.

If ImageBlocks are sent to a group of COSEM servers by broadcasting, the ImageBlockSize of each member in the group should be the same.

Step 2: The client initializes the mirror transmission.

The client initiates the image transfer process alone by calling the image_transfer_initiate method or uses broadcasting in all servers. The method calls parameter holds the identifier and the size of the Image to be transferred. The server should provide the memory space needed to accommodate the image.

After successful initialization, the value of the image_transfer_status attribute (1). The image _ transferred _ blocks _ status attribute should be reset, the value of the image _ first _ not _ transferred _ block _ number attribute should be set to 0, and the value of the image _ to _ activate _ info attribute should be reset. After the image transfer process is initialized, the COSEM server is ready to accept ImageBlocks.

Step 3: Client transmits ImageBlocks.

The client calls the image_block_transfer method by unicast or transmits the ImageBlocks to (a group of) servers by broadcast. The method calls parameters include ImageBlockNumber and an ImageBlock. Imageblock is only accepted by COSEM servers that have successfully started the image transmission process. Other servers will discard any ImageBlocks received.

Step 4: The client checks the integrity of the image.

The client checks the integrity of the transmitted image through each server. When receiving an upgrade packet, the meter associates the block number of the upgrade packet with the upgrade bitmap and determines whether the packet is lost based on the corresponding upgrade bit. The upgrade bitmap is as follows:

Bit order missing blocks																															
Byte	0								1								2								3							
Bit	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
Bit cum.	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8	23	22	21	20	19	18	17	16	31	30	29	28	27	26	25	24
Block available ?	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Hex value	FF								FE								FF								FF							
In this example Block number 8 is missing																																
NOTE!! The first blocknumber starts with 0 (zero)																																

If the mirror is not complete, it will transmit untransferred ImageBlocks. This is an iterative process, which lasts until the whole image is successfully transmitted.

There are two mechanisms available to identify and transmit untransmitted imageblock.

The client can retrieve the status of each ImageBlock: either there is no transmission, or it has been transmitted. This is performed by retrieving the value of the

image_transfer_blocks_status attribute. Then the client transmits the ImageBlocks that have not been transmitted.

Step 5: The server verifies the image.

The image is verified by the server. When making the meter upgrade package, the upgrade package will be encrypted by AES-GCM-128, and a 16-byte tag will be generated. The value of tag is placed at the end of the upgrade package. The client is started by calling the image_verify method, or it can be started by the server. The result can be:

- Success: If the verification can be completed.
- Temporary failure: if the verification is not completed.
- Other reasons: If the verification fails.

Step 6 (optional): The client checks the mirror information that needs to be activated. The client can check the result of image verification by retrieving the value of the image_transfer_status attribute. The value of this property will be updated as a result of image verification. A transmitted image can contain one or more images to be activated. For each image that is activated, this property contains parameters: {image_to_activate_size, image_to_activate_identification, image_to_activate_signature}.

Step 7: The server, using Upgrade client, activates the image Mirroring is activated by the server.

This can be initiated by the client calling the image_activate method or by the server. If activation is performed without prior verification, verification will be performed implicitly as part of activation. The result of calling the Image_activate method can be:

- Success means that the mirror activation has been successfully started.
- Temporary failure if verification/activation has not been completed.
- Other reason if activation fails.

If successful, the server will perform activation of the new image. In the process, it is inaccessible. After activating the Image, the client can check the result by retrieving the value of the image_transfer_status attribute or by reading the contents of the appropriate COSEM object containing the identifier, version, and digital signature of the activated firmware. Activate the command to restore the temporary fault.

Enforced SFR: FCS_COP.1/FW, FPT_TSU.1

7.7 Communication (SFR enforcing)

The communication is done according to Security Suite 0 and Security Policy 3. Security Policy 3 means that:

- (3) all messages to be authenticated and encrypted,

while Security Suite 0 will provide the following encryption algorithms:

Table 41 - Security Suite 0

Security	Suite name	Authenticated	Digital	Key	Hash	Key

Suite ID		encryption	signature	agreement		transport
0	AES-GCM	AES-GCM-128	-	-	-	AES key wrap 128 bit

The Optical Port, RS485 and Communication Module interfaces are using the same authentication and encryption methods, since those interfaces are using the same DLMS/Cosem architecture. Only the following (sections 7.7.1 – 7.7.4) interfaces are enabled on the device for communication.

Enforced SFRs by the Optical Port, RS-485 and Communication Module: FAU_ARP.2, FAU_GEN.1, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FAU_STG.3, FCS_CKM.4, FCS_COP.1/Auth, FCS_COP.1/FW, FCS_COP.1/GBE, FCS_COP.1/GUE, FCS_COP.1/KE, FCS_RNG.1, FDP_ACC.2, FDP_ACF.1, FDP_IFC.2/Int, FDP_IFC.1/Keys, FDP_IFC.1/Msgs, FDP_IFF.1/Int, FDP_IFF.1/Keys, FDP_IFF.1/Msgs, FDP_RIP.1, FIA_AFL.1, FIA_UAU.6, FMT_MOF.1, FMT_MTD.1/Audit, FMT_SMR.1, FMT_TMD.1/Time, FPT_BST.1, FPT_FLS.1, FPT_RPL.1, FPT_STM.1, FPT_TNN.1, FPT_TSU.1.

7.7.1 Optical Port

It can support bi-directional communication with HHU or PC software. The optical port on the meter cover has a Metallic ring inside. This interface complies with IEC 62056-21 MODE E and IEC 62056-46(HDLC). The baud rate for the opening sequence is 300bps and the baud rate to be proposed by the meter is 9600bps. It is used for local meter programming and data downloading, such as:

- Configure meter parameters.
- Reading data from meter, registers, Load profile, billing, event log etc.
- Update firmware.

Config communication parameter as follow:

- Protocol: IEC 62056-21 Mode E
- Port: according to the corresponding port on PC
- Baud Rate: 300 bps

7.7.2 RS485

It can support bi-directional communication with HHU or PC software. This interface complies with TIA/EIA-485-A and IEC 62056-46(HDLC). The baud rate for the communication is 9600 bps. It is used for local meter programming and data downloading, such as:

- Configure meter parameter.
- Reading data from meter, register, Load profile, billing, event log etc.
- Update firmware

7.7.3 Communication Module

The meter remote communicates with ARM system through communication module. Meter supports several types of communication modules, such as GPRS/4G, LTE-M. Module parameters can be set by PC software locally and also the ARM system remotely through DCU and Gateway. The P2P module can support both eSIM and SIM card Communication module upgrade supports locally by optical and remotely.

7.7.3.1 GPRS/4G module

The GPRS Module supports GSM; 4G Module supports GSM/LTE FDD. The specific description is as follows:

Table 42 - GSM module

Module	GSM	LTE FDD
Frequency bands	850/900/1800/1900MHz	B1/B3/B7/B8/B20
Transmission speed	Max 85.6 kbps(DL) Max 85.6 kbps(UL)	Max150 Mbps(DL) Max50 Mbps(UL);
Power	+33dBm (Power Class 4)	+23dBm (Power Class 3)
Work mode	Client/ server	Client/ server

7.7.3.2 LED operation

Table 43 - LED operation description

LED	Interval / State	Description
Power	Permanent ON	Module is powered on
	Permanent OFF	Module is powered off
Net	Permanent OFF	Module is not normal
	200ms ON, 1800ms OFF	Network searching, but register failed
	234ms ON, 266ms OFF	Network searching successful, standby state
	62ms ON, 63ms OFF	Data communication

7.7.3.3 LTE-M module

Toe has the following LTE-M key features:

- Cat-M supports: Band B1/B3/B5/B8/B20
- Single-Tone: uplink: 16.7kbps; downlink: 25.5kbps. λ Compliant with 3GPP REL. 13
- Support transparent data transmission and module can act as client.
- Internet Protocol Features: Support TCP protocols.
- Support firmware upgrade remotely and remote maintenance.
- Support firmware upgrade locally and local maintenance. λ USIM Interface: support USIM/SIM card: 3V,1.8V.
- The modem shall automatically register in the cellular network after power or mobile network coverage restoration or restart.

7.7.4 P1 Port

P1 Port is a read only interface. The meter has only one P1 port, the baud rate for the communication is 115200bps, using IEC 62056-21 mode D. The P1 port connector type is RJ12. The Metering System holds a female connector, the OSM (Other Service Module) connects via standard RJ12 male plug.

The P1 connector in the Metering System must be always accessible and should not be sealed or protected by a sealed cover. The P1 pin assignment is detailed in the table below:

Table 44 - P1 Pinout

Pin #	Signal name	Description	Remark
1	+5V	+5V power supply	Power supply line
2	Data	Data Request	Input

3	Data GND	Data ground	
4	n.c.	Not connected	
5	Data	Data line Output	Push–pull output
6	Power GND	Power ground	Power supply line

8 Acronyms

Table 45 – Terms and acronyms

Acronym	Meaning
4G	4G Wireless and International Mobile Telecommunication
AA	Application Associate
AARE	A-Associate Response – an APDU of the ACSE
AARQ	A-Associate Request – an APDU of the ACSE
AES-GCM-128	Advanced Encryption Standard - Galois/Counter Mode with 128 bit key
AK	Authentication Key
AMI	Advanced Metering Infrastructure
APDUs	Application Protocol Data Units
ARM	Automatic Meter Reading
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
client_SAP	client_Service Access Point
clientSAP	Client Service Access Point
COSEM	Companion Specification for Energy Metering
CRC	Cyclic Redundancy Check
CtoS	Client to Server
DC	Direct Current
DCU	Data Concentrator Unit
DL	Downlink
DLMS	Device Language Message Specification.
EAL	Evaluation Assurance Level
ECDSA	Elliptic Curve Digital Signature Algorithm
EEPROM	Electrically Erasable Programmable Read-Only Memory
EK	Encryption Key
F(CtoS)	Function (Client to Server)
F(StoC)	Function (Server to Client)
FIFO	First in first out
GBEK	Global Broadcast Encryption Key
GMAC	Message authentication code in Galois/Counter Mode
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GUEK	Global Unicast Encryption Key
HDLC	High-Level Data Link Control
HHU	Hand-Held Unit
HLS	High Level Security Authentication
IC	Integrated Circuit
IHD	In-Home Display
IoT	Internet of things
IRDA	Infrared Data Association
ISD	Infrastruktura Sieć Domowa (Polish)

IT	Information Technology
L1	Line 1
L2	Line 2
L3	Line 3
LCD	Liquid Crystal Display
LED	Light-Emitting Diode
LLS	Low Level Security Authentication
LLS	Low-Level Security
LTE-M	Long-Term Evolution Machine Type Communication
MCU	Microcontroller Unit
MK	Master Key
NB	Narrowband
NV	Non-volatile
OBIS	Object Identification System
OSP	Organizational Security Policy
PC	Personal Computer
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PLC	Power-line communication
PP	Protection Profile
PRNG	Probabilistic random number generator
RAM	Random Access Memory
RLRE	Release Response
RLRQ	Release Request
SA	Security Association
SAR	Security Assurance Requirement
server_SAP	server_Service Access Point
SFP	Security Functional Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
ST	Security Target
StoC	Server to Client
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
UL	Uplink
UTC	Coordinated Universal Time
VDEW	Verband der Elektrizitätswirtschaft (German Association of the Electricity Industry)
xDLMS	Extended Device Language Message Specification

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

[SX631] Smart Meter User Manual Model S34U28, date: 2024-07, version: v1.5

[SX601] Smart Meter User Manual Model S12U26, date: 2025-02, version: v1.6

[IEC 62056-21] INTERNATIONAL STANDARD IEC 62056-21 First edition 2002-05 Electricity metering – Data exchange for meter reading, tariff, and load control – Part 21: Direct local data exchange

[RS-485] Application Report SLLA070D–June 2002–Revised May 2010 RS-422 and RS-485 Standards Overview and System Configurations

[IEC 62056-46] INTERNATIONAL STANDARD IEC 62056-46 First edition 2002-02 Electricity metering – Data exchange for meter reading, tariff, and load control – Part 46: Data link layer using UDLC protocol

[B-Book] Blue Book Edition 14 - COSEM Interface Classes and OBIS Object Identification System DLMS UA 1000-1 Ed. 14, 2020-08-31

[G-Book] Green Book Edition 10 - DLMS/COSEM Architecture and Protocols DLMS UA 1000-2 Ed.10, 2020-08-31

[FIPS PUB 197] Federal Information Processing Standards Publication Advanced Encryption Standard (AES) Published November 26, 2001; Updated May 9, 2023

[AGD] AGD Documentation SANXING SX601 and SX631 Smart Meters, v1.7, 2025-11-04

[OBIS_LIST] OBIS_HU_V2.2 20250620.xlsx

[DSMR-P1] P1 Companion Standard Dutch Smart Meter Requirements - Netbeheer Nederland – WG DSMR, version: v5.02, date: 2016-02-16

[EQ-Report] Equivalency report SANXING SX601 1-phase and SX631 3-phase Smart Meter, v1.2, 2025-05-28