Federal Office
for Information Security

Protection Profile for a Smart Meter Gateway (SMGW-PP)

Version 2.0

Certification-ID: BSI-CC-PP-0073-V2

13.12.2024

Bundesamt für Sicherheit in der Informationstechnik
PO Box 20 03 63
53133 Bonn
E-Mail: smartmeter@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

List of Figures

List of Tables

1 PP introduction

1.1 Introduction

The renewable energy transition entails a de-centralization of energy production and the need for automated, digitized coordination of generation, storage and consumption of energy. An adjustment of the grid towards not only small, de-centralized production plants but also energy storage systems as well as flexible consumption devices is therefore necessary. This requires a transformation in particular of low- and medium-voltage networks of the grid to a *smart grid*, i.e., a *commodity* network, that intelligently integrates the behaviour and actions of all entities connected to it. This efficiently ensures a more sustainable, economic and secure supply of that commodity. Entities of the smart grid may be suppliers of natural resources and energy, its *consumers* and those that are both, as well as energy storage systems.

The smart grid needs to allow for the flexibility to coordinate consumption and production of its commodity: A smart grid has to enable the integration of consumer devices that regulate the load and availability of resources or energy in the grid.

To provide this integration of flexibly controllable production and consumption devices, the *smart metering system* is essential. It measures the consumption or production of certain commodities at the consumers' side and further allows sending this information to *external entities* as basis for e.g. the billing of consumption or production. In addition, it provides the possibility to support the controlling of production and consumption devices. Finally, it provides a transparent means of information by providing an interface for consumers and their devices to access data associated with them.

This *protection profile* (PP) defines the security objectives and corresponding requirements for a *smart meter gateway* (SMGW), which is the central communication component of a smart metering system (please refer to chapter ▸Section 1.4.2 for a more detailed overview). The PP is directed to developers of SMGWs and contains the requirements that have to be met. It is further directed to *metering point operators* (MPOs) responsible for operating SMGWs. Note that in addition to the security requirements of this PP, [BSI-TR-03109-1] defines interoperability and functional requirements for SMGWs.

The *target of evaluation* (TOE) that is described in this document is an electronic unit comprising hardware and software/firmware[1] used for collection, processing, storage and provision of meter data from one or more meters of one or multiple commodities. It connects a *wide area network* (WAN) with a network of devices of one or more *meters* (*local metrological network*, LMN) and the *home area network* (HAN). In the HAN, the TOE provides access for consumers and communication with controllable local systems or devices for value-added services (cf. the term *CLS* in ▸Section 3.1). The TOE supports the controlling of such controllable local systems. The security functionality of the TOE comprises in particular

- the protection of *confidentiality*, *authenticity*, *integrity* of data and
- information flow control,

mainly to protect the privacy of consumers, to ensure a reliable billing process and to protect the smart metering system and a corresponding large-scale infrastructure of the smart grid. The TOE is part of the device SMGW and relies on the functionality of a *security module* (which is part of the SMGW but not of the TOE) for parts of its security functionality. For the precise boundary of the TOE see ▸Section 1.4.5 and ▸Section 1.4.6. The availability of the TOE is not addressed by this PP.

By the collection, processing and storage of meter data by SMGWs, the decentralized approach as required by [MsbG] is implemented. *Meter data* are sent to *external market participants* e.g. for billing purposes, but are also made available locally in the HAN to the consumers and their devices as well as to CLS devices.

SMGWs support controlling of CLS devices in the HAN in the following way: As a mandatory functionality, the SMGW provides a *TLS* proxy functionality between CLS devices in the HAN and external market participants in the WAN. This TLS proxy channel may be used to send data from an external market participant to a CLS device. The contents of this TLS proxy channel are transparent to the SMGW and may contain control commands. In addition, as an optional functionality, *control data* may be sent by the *gateway administrator* (GWA) to the TOE, which stores, possibly processes and sends them to CLS devices for further usage. Infor-

[1] For the rest of this document the term “firmware” will be used.

mation on these control data is then available for consumers in the HAN. The SMGW may further process control data in combination with meter data to realize further funtionalities. If this optional functionality is implemented in the SMGW, the functional package "power limitation" as described in ▸Section 7.2 shall be included in the *security target* (ST).

SMGWs include a functionality to remove *personally identifiable information*, thus allowing a de- and re-installation at a different location, and contributing to sustainability.

The TOE as described in this PP is assumed to be installed behind a *grid connection point*, and assumed to connect meters as well as CLS devices associated with that grid connection point. Optionally, the SMGW may also be installed to connect meters as well as CLS devices from multiple grid connection points within one grid node of the same voltage level. If the SMGW is intended for that usage, the functional package "multiple grid connection points" as described in [Package_MultipleGcp] shall be included in the *security target* (ST) of the developer.

1.2 PP Reference

Title	Protection Profile for a Smart Meter Gateway (SMGW-PP)
Version	2.0 (Release Candidate)
Date	2024-11-29
Sponsor	Federal Office for Information Security, Germany
Registration	BSI-CC-PP-0073-V2
Assurance Level	*EAL*4 augmented by AVA_VAN.5 and ALC_FLR.2
CC Version	CC:2022 Revision 1
Keywords	smart metering, smart grid, protection profile, meter, gateway, PP

1.3 Specific terms

Various vocabularies exist in the area of smart grid, smart metering and home automation. Further, the Common Criteria (CC) maintain their own vocabulary. For a glossary and list of acronyms see ▸Glossary.

Application Note 1: This PP makes use of application notes. Application notes are a means to provide the ST author with information on how to design the ST. Application notes shall be adhered to during the generation of an ST. Application notes that have been addressed or that do not apply for the TOE shall not be present in the ST. For more information, see [AIS32].

1.4 TOE overview

1.4.1 Introduction

The TOE of this PP is the part of the SMGW that comprises the hardware and firmware that is relevant for the security functionality of the SMGW as defined in the following. Note that the SMGW contains a security module that is not part of the TOE. The precise boundary of the TOE is given in ▸Section 1.4.5 and ▸Section 1.4.6.

In the following sections, the SMGW (containing the TOE) as part of a smart metering system, as well as the communication of the SMGW with external entities will be described.

1.4.2 Overview over the SMGW in a smart metering system

▸Figure 1.1 provides an overview of the TOE as part of an SMGW with the networks it connects from a purely functional perspective as used in this PP.[2]

[2] It should be noted that this description purely contains aspects that are relevant to motivate and understand the functionalities of the SMGW as described in this PP. It does not aim to provide a universal description of a smart metering system for all application cases.

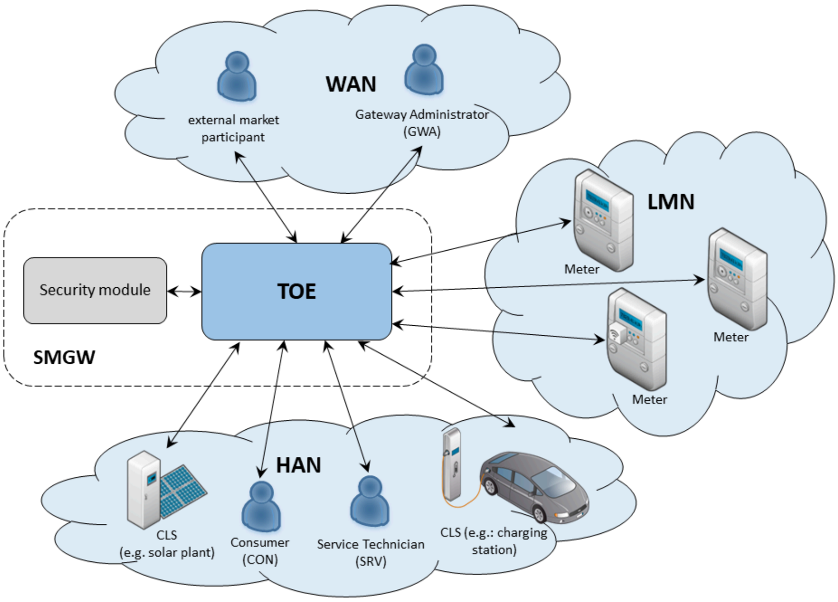


Figure 1.1. The TOE and its direct environment

A smart metering system comprises different functional units in the context of the descriptions in this PP:

- The **SMGW** (as defined in this PP) serves as the communication component between devices in the LMN and HAN of the consumer (such as meters and added generation plants) and the outside world. It can be seen as a kind of firewall dedicated to the smart metering functionality. It collects, processes, and stores the records from meter(s) as well as derivatives thereof and ensures that only authorized parties have access to them. Before transmitting meter data[3] via the WAN interface, the information will be encrypted and signed using the services of a security module.

  Additionally, the SMGW supports the controlling of CLS devices via the TLS proxy functionality. Optionally, the SMGW is capable to collect, process, store and forward control data. It may receive control data receipts from CLS, as well as internally process and forward the receipts or results, see ▸Section 7.2.

  Further, the SMGW features a mandatory local interface for authorized consumers to access the data relevant to them. It further offers a local interface to *service technicians* (SRV) for diagnostic purposes. Note that the TOE of this PP is part of the SMGW, but the SMGW contains parts that are not included in the TOE, such as the security module, see also ▸Section 1.4.5.

- The ***meter*** itself records the consumption or production of one or more commodities (e.g., electricity, gas, water, heat) and submits those records in defined intervals to the SMGW. These meter data have to be signed and encrypted by the SMGW before transmission to external entities in order to ensure its confidentiality, authenticity, and integrity. The meter is comparable to a classical meter[4] and has comparable security requirements; it will be sealed as classical meters according to the regulations of the calibration authority. The meter further supports the encryption and integrity protection of its *connection* to the SMGW[5]. Meter is a hypernym for *residential meters* and *industrial meters* in the LMN, the difference of those being that data of industrial meters are associated with a legal entity and are not considered personally identifiable information.

[3] Please note that readings and data that are not relevant for billing may require an explicit endorsement of the consumer.

[4] In this context, a classical meter denotes a meter without a communication channel, i.e. whose values have to be read out locally.

[5] It should be noted that this PP does not imply that the connection between the SMGWs and external components (specifically meters and CLS) is cable-based. It is also possible that the connections as shown in ▸Figure 1.1 are realized deploying a wireless technology. However, the requirements on how the connections shall be secured apply regardless of the realisation.

Residential meters are only located in the LMN. Industrial meters may be located in the LMN or in the HAN. However, in the case of being located in the HAN, they do not fall under the hypernym **meter** and the data generated and sent to the SMGW are not considered meter data. Instead, industrial meters in the HAN are considered to be CLS, see below.

- The SMGW utilizes the services of a **security module** (e.g., an integrated chip) as a cryptographic service provider and as a secure storage for private keys and possibly further confidential assets. The security module is contained in the SMGW but it is not part of the TOE of this PP; it is evaluated separately according to the requirements in the corresponding PP (c.f. [SecMod-PP]).

CLS (as shown in ▸Figure 1.2) are located in the HAN. They may range from local power generation plants, controllable loads such as heat pumps, electronic vehicle chargers or battery storage to applications in home automation. In addition, devices for value-added services, such as heat cost allocators, as well as industrial meters in the HAN of the SMGW are summarized under the term CLS for simplicity. CLS may utilize the services of the SMGW for communication services, to receive control data from the SMGW or to obtain the legal time-base from the SMGW.

The following ▸Figure 1.2 introduces the minimum required physical interfaces of the TOE and shows the cardinality of the involved entities. [6]

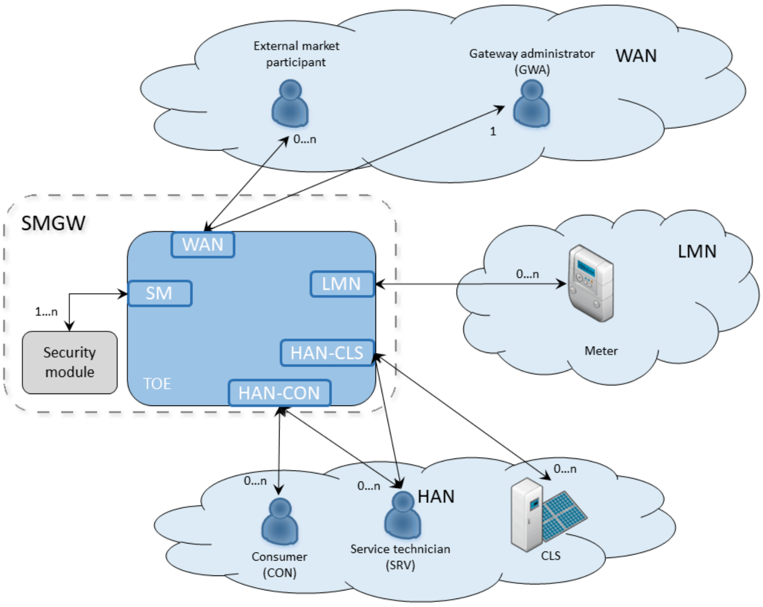


Figure 1.2. The physical interfaces of the TOE and the cardinality of the involved external entities.

Please note that the arrows of the physical interfaces as shown in ▸Figure 1.2 indicate the flow of information. However, they do not indicate that a communication flow can be initiated bi-directionally. Indeed, this PP will place dedicated requirements on the way an information flow can be initiated.

As ▸Figure 1.2 indicates, the TOE provides at least two physical interfaces HAN-CON and HAN-CLS to the local network referred to as "HAN". All services of the TOE provided at HAN-CLS are also provided at HAN-CON and vice-versa.

Application Note 2: A separation of the HAN into two networks HAN-CON and HAN-CLS is not required by this PP. If such a separation is enforced by a TOE, the ST author shall adjust the information in the ST and model this functionality accordingly. In case such a separation is provided by the TOE, still all services that are provided in the HAN as described in this PP and in [BSI-TR-03109-1] have to be provided at the TOE's interfaces to both networks.

The overview of the smart metering system as described before is based on a threat model that has been developed for the smart metering system and that is motivated by the following considerations:

[6] Note that during the switch of a GWA for a TOE, the cardinality of GWAs interacting with one SMGW may be two for a short period of time. However, except for this case, only one GWA exists for a TOE.

- The SMGW is the central communication unit in the smart metering system. It shall be the main unit directly connected to the WAN.
- The SMGW is the central component that collects, processes, and stores meter data and supports the controlling of CLS devices. It is therefore the primary point of *user* interaction in the context of the smart metering system.
- To conquer a meter in the LMN, a remote attacker first would have to attack the SMGW successfully. All data transferred between LMN and WAN flows via the SMGW, which makes it an ideal unit for implementing significant parts of the system's overall security functionality.
- To conquer a device in the HAN (a consumer device or a CLS), a remote attacker would either have to attack the SMGW successfully, attack a device in the HAN with a separate connection into another network, or would have to attack the device directly. The security of these devices is not part of the evaluation of this PP. However, it is assumed that in particular those devices with a separate connection into another network have an appropriate level of protection.[7]
- Because an SMGW can be used to connect and protect multiple meters (while a meter will always be connected to exactly one SMGW) and CLS with the WAN, there might be more meters and CLS in a smart metering system than there are SMGWs.
- The SMGW is located within a physical casing, where the casing itself is also part of the TOE. Nevertheless, some physical and logical components within the casing might be non-TOE, as long as those do not realize any kind of security-relevant functionality defined in ▸Chapter 6. In particular, the security module contained within the casing is not part of the TOE.
- The SMGW as well as the connected meters and CLS lie within the same *premises*.

All these arguments motivated the approach to have an SMGW (using a security module for cryptographic support), which is rich in security functionality, strong and evaluated in depth, in contrast to a meter which will only deploy a minimum of security functions. The security module will be evaluated separately.

It should be noted that this PP does not aim to imply any specific system architecture or product design as long as the security requirements from this PP are fulfilled. Only in cases where the implementation of the security functional requirements (SFRs) will require a certain architecture, this architecture is described in this PP in a mandatory way. To underline this approach, this PP will further refer to the term “unit” whenever the TOE or another part of the smart metering system is described from a functional perspective and only use the term “component” or “device” when a real physical device is described. Possible forms of implementing the units of a smart metering system in components are described in ▸Section 1.4.5.

1.4.3 TOE description

The TOE as part of an SMGW within the smart metering system serves as the communication unit between devices of consumers and service providers of a commodity industry (e.g., electricity, gas, water, heat). It also collects, processes, and stores meter data and is responsible for the distribution of this data to external market participants as well as to consumers and devices in the HAN.

The TOE as part of an SMGW enables access to local meter(s) (i.e., the unit(s) used for measuring the consumption or production of electricity, gas, water, heat) and may enable access to CLS (e.g., power generation plants, controllable loads such as heat pumps, EV chargers, battery storage or devices for value-added services). Roles respectively external entities in the context of the TOE are introduced in ▸Section 3.1.

The TOE as part of the SMGW has a fail-safe design that specifically ensures that any malfunction cannot impact the delivery of a commodity, e.g., energy, gas or water.

[7] A certification according to [BSI-TR-03109-5] provides a means to achieve this appropriate level of protection. Note that not all devices in the HAN fall under the scope of [BSI-TR-03109-5]. For devices that are not addressed by [BSI-TR-03109-5], still an appropriate level of protection is required.

1.4.4 TOE type

The TOE is a communication gateway. It provides different external communication interfaces and enables the data communication between these interfaces and connected IT systems. It further collects, processes, and stores meter data and supports the controlling of CLS devices.

1.4.5 TOE physical boundary

1.4.5.1 Introduction

The TOE comprises the hardware and firmware that is relevant for the security functionality of the SMGW as defined in this PP. The security module that is utilized by the TOE is contained in the SMGW, but it is not part of the TOE.

This PP does not imply any physical architecture for the components that make up the smart metering system. The following sections introduce examples of physical representations for the different components of the smart metering system – focusing on the TOE.

It should be noted that this overview of possible physical implementations does not claim to be complete.

1.4.5.2 Possible TOE design

The following ▸Figure 1.3 provides an example for an implementation of the TOE and its relation to the physical device SMGW as defined in this PP.

An SMGW is a device comprising at least:

- the security relevant parts (i.e., TOE security functionality (TSF)) of the TOE,
- a *communication adapter*[8] responsible to provide access to a connected network (may be part of the TOE but shall be part of the physical device), and
- the security module that is not part of the TOE.

Note that [BSI-TR-03109-1] addresses further (non-security-relevant) requirements for the SMGW that have to be adhered to.

The TOE communicates with one or more meters in the LMN, provides an interface to the WAN and provides two physical interfaces HAN-CLS and HAN-CON to the network HAN.

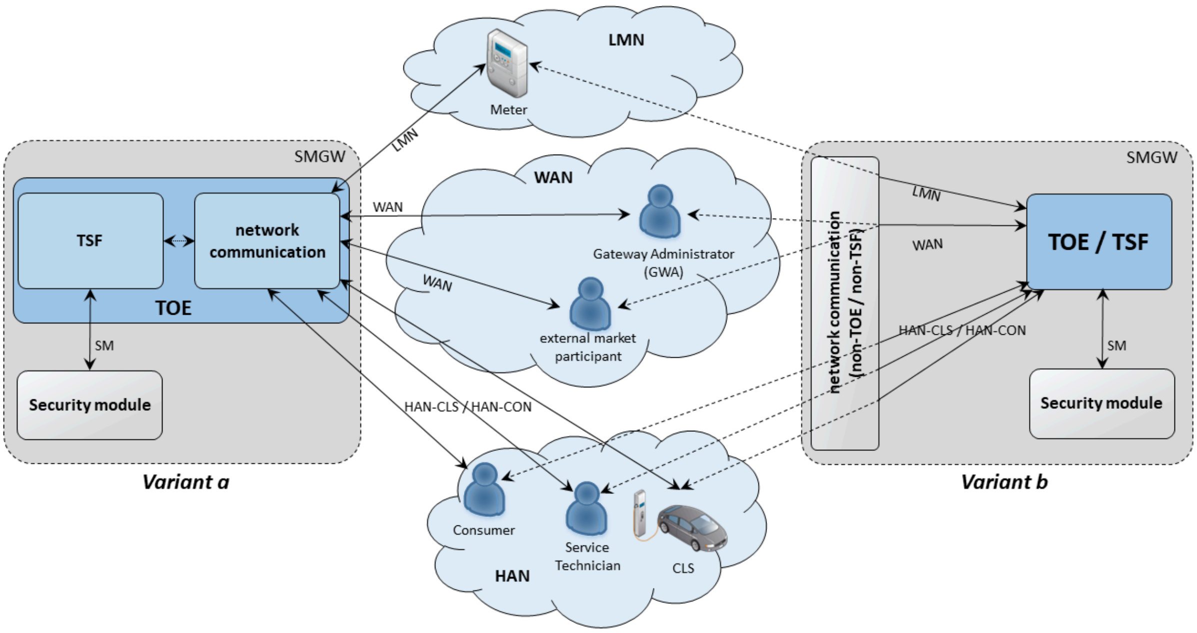


Figure 1.3. TOE design

[8] Please note that this refers to the pure communication services excluding encryption functionality.

Different layouts may be used concerning the relation between the communication adapter and the TOE, as depicted in ▸Figure 1.3). *Variant a* follows the approach to include the communication services within the logical TOE boundary and hence into the scope of the PP. *variant b* uses a communication adapter outside the TOE scope to set up a subset or all communication links to WAN, LMN or HAN. Hence, the TOE security functionality interfaces (TSFIs) of the SMGW might be at the physical boundary of the casing (in *Variant a*) or at internal interfaces within the casing (in *variant b*).

1.4.5.3 Additional TOE configurations due to second source strategies for hardware components

In general, the modification, exchange or removal of an existing component and the inclusion of a new one leads to a new TOE configuration.

In order to provide the developer with the necessary flexibility in terms of second source and security design strategies, this does not apply to passive components (such as resistors or capacitors).

However, the modification, exchange, removal or inclusion of all non-passive components (such as CPU, RAM or flash) or directly security-relevant ones (such as the seal) leads to a further TOE configuration. This also holds for the security module.

1.4.6 TOE logical boundary

1.4.6.1 Overview over TOE security features

The logical boundary of the TOE can be defined by its security features:

1. **Handling of meter data**: The collection and processing of meter data, submission to authorized external market participants (e.g., one of the service providers involved), where necessary protected by a digital signature.
2. **Protection** of **authenticity**, **integrity** and **confidentiality** of data temporarily or persistently stored in the TOE, transferred locally within the LMN or HAN and transferred in the WAN (between TOE and authorized external entities).
3. **Firewalling** of information flows to the WAN and **information flow control** among meters, CLS and the WAN.
4. A **wake-up-service** that allows to contact the TOE from the WAN side.
5. **Privacy preservation**.
6. The **management** of security functionality.
7. The **identification and authentication** of TOE users.
8. A **Key generation service** for external entities.

Application Note 3: Please note that it is possible that the TOE provides more functionality than required by this PP. However, all additional functionality of the TOE has to be implemented in a way that it cannot impact the security functionality required by this PP.

Application Note 4: The provision of software updates for meters in the LMN or CLS in the HAN is included implicitly in this PP. Software updates are part of the asset meter config or CLS config, respectively. The read access and the management are modelled in the respective SFRs in ▸Chapter 6. If the functionality is implemented in the TOE, the ST author shall describe the functionality of the TOE in the TOE summary specification.

Note that in case this functionality is described and detailed in [BSI-TR-03109-1], the ST author shall model the functionality in this PP consistently with the requirements therein. Further information may be provided in accompanying documents to [BSI-TR-03109-1].

Application Note 5: The TOE may support controlling of CLS in two ways. Either the control commands are sent via the TLS proxy channel to CLS. In this case, the control commands are part of the asset supplementary data, see ▸Section 3.2. Or the control data may be sent by the GWA to the TOE, which stores, possibly processes and then sends them to a CLS. In the latter case, the ST author shall model the functionality of the TOE using the functional package defined in ▸Section 7.2.

Note that in case this functionality is described and detailed in [BSI-TR-03109-1], the ST author shall model the functionality in this PP consistently with the requirements therein. Further information may be provided in accompanying documents to [BSI-TR-03109-1].

The ST author shall add the information concerning this functionality in ▸Section 1.4.3 and in this section as a separate security feature.

The following sections introduce the security functionality of the TOE in more detail.

1.4.6.2 Handling of meter data[9]

The TOE is responsible for handling meter data. It receives the meter data from the meter(s) in the LMN, processes it, stores it and submits it to external market participants.

The TOE utilizes processing profiles to determine which data shall be sent to which external entity defined in chapter ▸Section 3.1. A processing profile defines:

- from which meter the meter data originate,
- how meter data must be processed,
- which processed meter data must be sent in which intervals,
- what external entity is the designated recipient of the processed meter data,
- which key material is used for signing the processed meter data,
- which key material is used for encryption (if any),
- whether processed meter data shall be pseudonymized or not, and if yes,
- which pseudonym shall be used to send the data.

Processing profiles are the basis for the security features of the TOE concerning the handling of meter data and they define how the meter data shall be processed. Processing profiles shall be visible for the consumer to allow a transparent communication. It is essential that processing profiles correctly define the amount of information that must be sent to an external market participant. More details on processing profiles, also on the non-security-relevant functionality, can be found in [BSI-TR-03109-1].

Please note that it is possible that a TOE enforces more than one processing profile, specifically if the communication and the contractual requirements for multiple external entities have to be handled. Note that only those processing profiles are permitted which are realized according to [BSI-TR-03109-1] or which are defined in accompanying documents to [BSI-TR-03109-1]. Further processing profiles are not permitted and shall not be accepted by the TOE.

The TOE will restrict access to (processed) meter data in the following ways:

- consumers shall be identified and authenticated before access to any data may be granted,
- the TOE shall accept meter data from authorized meters only,
- the TOE shall send processed meter data to correspondingly authorized external market participants only.

The TOE shall accept data (e.g., configuration data, *firmware updates*) from correspondingly authorized GWAs or correspondingly authorized external entities only. This restriction is a prerequisite for a secure operation and therewith for a secure handling of meter data. Further, the TOE shall maintain a calibration log with all relevant events that could affect the calibration of the TOE.

The TOE allows the consumer in the HAN to obtain information via both physical interfaces HAN-CON and HAN-CLS. This information comprises the billing-relevant data (to allow the consumer to verify an invoice) and information about which meter data has been and will be sent to which external market participant.

[9] Please refer to chapter ▸Section 3.2 for an exact definition of the various data types.

The TOE ensures that the communication to the consumer is protected and ensures that consumers only gain access to the data they are associated with. Please note that accessing this interface by the consumer may happen via different technologies as long as the security requirements are fulfilled. The TOE's physical interfaces to the HAN (HAN-CON and HAN-CLS) may be used by a remote display dedicated to this purpose or may be accessed e.g. via a PC-based web browser[10].

This functionality shall

- prevent that the TOE accepts data from or sends data to unauthorized external entities,
- ensure that only the minimal amount of data leaves the scope of control of the consumer[11],
- preserve the integrity of customer billing, network-usage billing, and balancing processes and as such serve the interests of consumers, suppliers, network operators, and are fundamental to the stability of the energy system,
- preserve the integrity of the components of the smart metering system and their configurations.

1.4.6.3 Confidentiality protection

The TOE protects data from unauthorized disclosure

- while received from or transmitted to an external entity via the WAN, LMN or HAN,
- while stored temporarily in the volatile memory of the TOE,
- while stored persistently in the memory of the TOE.

Furthermore, all data, which no longer have to be stored in the TOE, are securely erased to prevent any form of access to residual data via external interfaces of the TOE.

This functionality shall protect the privacy of the consumer and shall prevent that an unauthorized party is able to disclose any of the data transferred to and from the smart metering system (e.g., meter data, configuration settings).

The TOE utilizes the services of its security module for aspects of this functionality.

1.4.6.4 Integrity and authenticity protection

The TOE shall provide the following authenticity and integrity protection:

- Verification of authenticity and integrity when receiving meter data from a meter via the LMN, to verify that the meter data have been sent from an authentic meter and have not been altered during transmission.
- Application of authenticity and integrity protection measures when sending processed meter data to an external market participant, to enable the external market participant to verify that the processed meter data have been sent from an authentic TOE and have not been changed during transmission.
- Verification of authenticity and integrity when receiving data from an external entity (e.g., configuration settings or firmware updates) to verify that the data have been sent from an authentic and authorized external entity and have not been changed during transmission.

The TOE utilizes the services of its security module for aspects of this functionality.

This functionality shall:

- prevent within the smart metering system that data may be sent by a non-authentic component without the possibility that the data recipient can detect this,
- facilitate the integrity of customer billing, network-usage billing, and balancing processes and as such serve the interests of consumers, suppliers, network operators and other parties that provide services in the en-

[10] Please note that the access to the TOE via a device that has a separate connection to the WAN may incur a scenario for data leakage if that device is not adequately protected.

[11] This PP does not define the standard on the minimal amount that is acceptable to be submitted. The decision about the frequency and content of information has to be considered in the context of the contractual situation between the consumer and the external entities.

ergy system on the basis of meter values. All parties are interested in the transmission of correct processed meter data to be used for billing and/or stabilization of the energy system.

- protect the smart metering system and a corresponding large scale smart grid infrastructure by preventing that data (e.g., meter data, configuration settings, or firmware updates) from forged components (with the aim to cause damage to the smart grid) will be accepted by the TOE.

1.4.6.5 Information flow control and connection establishment

The TOE shall separate devices in the respective networks from each other and shall enforce the following rules for information flow control and *connection establishment* to control the communication between the networks that the TOE is attached to:

- information flow is only allowed to and from authorized external entities and via a trusted channel,
- information flow of meter data is directed by information in processing profiles,
- the TOE can establish connections to devices in the WAN, LMN or HAN,
- connection establishment to the TOE initiated by external entities in the WAN shall be denied,
- a CLS in the HAN may establish a connection to an external market participant in the WAN via the TOE as proxy[12]; an external market participant may not establish such a connection themselves, instead, they require the GWA to administer a channel establishment initiated by the TOE to the external market participant as well as to the CLS,
- the TOE shall offer a wake-up service that allows the GWA in the WAN to trigger a connection establishment, see ▸Section 1.4.6.6,
- TLS endpoints of communication channels from or to the TOE shall exist in the TOE itself and at roles/entities defined in ▸Table 3.1 only,
- connections are allowed as defined in communication profiles only,
- only cryptographically protected, i.e., encrypted, integrity protected and mutually authenticated, connections are possible.[13]

This functionality shall:

- prevent that the TOE itself or the components behind the TOE (i.e., meters or CLS) can be conquered by a remote attacker via the TOE (as defined in ▸Section 3.4), that processed data are transmitted to the wrong external entity, and that processed data are transmitted without being protected according to their specific need,
- protect the smart metering system and a corresponding large scale infrastructure in two ways: by preventing that conquered components will send forged meter data (with the aim to cause damage to the smart grid), and by preventing that widely distributed smart metering systems can be abused as a platform for malicious software to attack other systems in the WAN (e.g., a remote attacker who would be able to install a botnet on components of the smart metering system).

The limitation on communication flows that is enforced by the TOE between parties in the WAN, LMN and HAN is depicted in ▸Table 1.1.

[12] Technically, this channel is established by the TOE who acts as a proxy between the CLS and the external entity in the WAN.

[13] To establish an encrypted channel, the TOE may use the required protocols such as DHCP or PPP. Beside the establishment of an encrypted channel, no unprotected communication between the TOE and external entities located in the WAN, LMN or HAN is allowed. Note that communication with unidirectionally communicating meters cannot be mutually authenticated; in addition, receiving the *SMGW time* from the SMGW does not require authentication from the respective external entities in HAN or LMN.

Destination Source	WAN	LMN	HAN
WAN	Communication within the **WAN** is not restricted. However, the TOE is not involved in this communication.	No connection establishment is allowed.	No connection establishment is allowed.
LMN	No connection establishment is allowed.	No communication between devices in the **LMN** is assumed. It is assumed that residential meters in the LMN only communicate with the TOE and are not be connected to any other network; industrial meters in the LMN are assumed to only have additional unidirectional (outbound) connections to other networks.	No connection establishment is allowed.
HAN	No connection establishment is allowed.	No connection establishment is allowed.	Devices in the HAN may communicate with each other. However, the TOE is not involved in this communication. If devices in the HAN have a separate connection to parties in the WAN (beside the TOE), this connection is assumed to be appropriately protected.

Table 1.1 Limitation on communication flows enforced by the TOE between different entities in the WAN, LMN and HAN

The TOE itself shall offer the following services to external entities within the various networks:

1. WAN:
   a. the TOE shall offer management functionality to the GWA,
   b. the TOE shall send meter data to external market participants according to the processing profiles,
   c. the TOE shall offer a wake-up service to the GWA,
   d. the TOE shall provide the possibility for the GWA to use a wake-up to initiate a TLS proxy channel between an external market participant in the WAN and a CLS in the HAN.
2. LMN:
   a. the TOE shall accept the submission of meter data from devices in the LMN,
   b. the TOE shall offer a key generation service for devices in the LMN,
3. HAN (accessible via the physical interfaces HAN-CON and HAN-CLS):
   a. the TOE shall provide consumers access to their respective consumer logs and to the management functionality,
   b. the TOE shall provide SRVs access to the system log and to the management functionality,
   c. the TOE shall offer a key generation service for CLS,
   d. the TOE shall provide the SMGW time to devices in the HAN,
   e. the TOE shall provide the TLS proxy functionality to CLS in the HAN, i.e., the possibility to establish a trusted channel to an external market participant.

1.4.6.6 Wake-up service

In order to protect the TOE and the devices in the LMN and HAN against threats from the WAN, the TOE implements a strict firewall policy and enforces that connections with external entities in the WAN shall only be established by the TOE itself (e.g., when the TOE delivers meter data or contacts the GWA to check for updates)[14].

While this policy is the optimal policy from a security perspective, the GWA might require an instant communication to the TOE for certain applications. In addition, an external market participant might require an instant communication to the TOE to communicate with a CLS using the SMGW's TLS proxy functionality. In order to allow this kind of responsiveness of the TOE, this PP allows the TOE to keep existing connections to external entities open (please refer to [BSI-TR-03109-3] for more details) and to offer a so-called wake-up service to the GWA.

The TOE shall be able to receive a wake-up message that is signed by the GWA. This information contains in particular whether the SMGW shall establish a connection to the GWA, or to an external market participant and to a CLS to establish a TLS proxy channel between those external entities. The implementation shall follow the description in [BSI-TR-03109-1]. Further information may be provided in accompanying documents to [BSI-TR-03109-1].

1.4.6.7 Privacy preservation

The preservation of the privacy of the consumer is an essential aspect that is implemented by the functionality of the TOE as required by this PP. This contains two aspects:

The processing profiles facilitate an approach in which only a minimal amount of data has to be submitted to external market participants and therewith leave the scope of control of the consumer. The mechanisms “encryption” and “pseudonymization” ensure that the data can only be read by the intended recipient and and any association with the identity of a meter may be removed if necessary.

On the other hand, the TOE shall provide the consumer with transparent information about the information flows containing their data. To this extent, the TOE shall implement a consumer log that contains information about the information flows that have been and will be authorized based on the previous and current processing profiles. The access to this consumer log is only possible via HAN-CLS or HAN-CON and after authentication of the consumer. The TOE shall only allow a consumer access to the data in the consumer log that is related to devices they are associated with. The following paragraphs provide more details on the information that shall be included in this log:

Monitoring of data transfers

The TOE shall be able to keep track of data transmission in the consumer log and allow the consumer to see details on which information has been and will be sent (based on the previous and current settings) to which external entity.

Configuration reporting and monitoring

The TOE shall provide detailed and complete reporting of each security and privacy-relevant configuration setting. In addition to device-specific configuration settings, the consumer shall be able to obtain information on the parameters of each processing profile. Further, the consumer shall be able to read the configured addresses for internal and external entities including the CLS associated with that consumer. The consumer log provides the consumer with

- the consumer's user identity,
- the TOE version (including hardware and software version) and identity,
- identities of meters and of external entities in the WAN that are allowed to receive meter data associated with the consumer's user id,
- information about information flows of meter data associated with the consumer's user identity to external entities in the WAN,
- information about status events and errors relevant for the consumer,

[14] Please note that this does not affect the functionality for a CLS to establish a secure channel to an external market participant in the WAN. Technically however, the part of the TLS proxy channel between the TOE and the external market participant is established by the TOE.

- information about management and configuration of attributes, data, processing profiles and communication profiles associated with the consumer's user identity.

The TOE shall provide all audit data from the consumer log at the interfaces HAN-CON and HAN-CLS. Access to the consumer log shall only be possible after successful authentication and only to information that the respective consumer has permission to (i.e., that has been recorded based on events related to that consumer's data).

User data reset

The TOE shall provide a user data reset functionality for the authorized GWA at the interface WAN and for the authorized SRV at the interfaces HAN-CON and HAN-CLS. This functionality renders the following data and information irreversibly inaccessible:

- communication profiles for CON, LMN, external market participants and proxy communication profiles
- processing profiles
- meter data
- system log data
- consumer log data
- calibration log data except for events on successful firmware updates of the TOE
- further personally identifiable information (PII)

The user data reset functionality shall be used by the authorized GWA and the authorized SRV prior to a de-installation of the SMGW followed by a re-installation at another location. Note that, if necessary, an export of data may be required prior to the usage of the user data reset functionality.

1.4.6.8 Management of security functions

The TOE provides management functionality with which authorized GWAs can monitor and configure all aspects of the TOE. In addition, it provides limited management functionality for authorized SRVs and consumers, as well as specific management services for meters and CLSs. This PP defines a minimal set of management functions that must be implemented by each TOE seeking conformance to this PP.

The majority of the management functionality of the TOE is only accessible to an authorized GWA. In particular, only the GWA may update the TOE. The authorized SRV may manage *WAN communication parameters* as well as initiate a self-test, a restart or a user data reset of the TOE.

Further services provided by the TOE that may be initiated by authorized external entities other than the GWA, which may be considered management functionality are

- by a consumer: the change of their own password,
- by a CLS: the establishment of a trusted communication channel with an external market participant, and
- by a CLS or meter: the initiation of the generation of a public-private-key pair by the TOE.

The TOE shall provide information on the status of the TOE in the system log. Specifically, it shall indicate whether the TOE operates normally, or whether any errors have been detected that are of relevance for the GWA. The system log shall be accessible by the GWA and the SRV.

1.4.6.9 Identification and authentication

To protect the TSF as well as user data and TSF data from unauthorized access, disclosure or modification, the TOE provides a mechanism that requires each user to be successfully identified and authenticated before allowing any other TSF-related actions on behalf of that user. This functionality includes the identification and authentication of users who receive data from the TOE as well as the identification and authentication of CLS located in the HAN and meters located in the LMN. As an exception, external entities in the HAN and LMN may receive the SMGW time from the TOE without authenticating themselves to the TOE.

The TOE provides different kinds of identification and authentication mechanisms that depend on the user role and the used interfaces. The usage of certificates is required for all roles and interfaces except for unidirectionally communicating meters in the LMN (communication using wM-Bus), and for consumers at HAN-CON and HAN-CLS, as they may choose between the usage of certificates or user id and password.

1.4.6.10 Key generation service

The TOE provides a key generation service for CLS and meters. This functionality comprises

- the generation of a private-public key pair and a corresponding self-signed certificate and
- the generation of a shared, meter-individual key for meters in the LMN.

The TOE utilizes the services of its security module for the random number generation of this functionality.

1.4.7 The interfaces of the TOE

The TOE offers its functionality via a set of external interfaces. The TSFIs are located at the logical TOE boundary by definition. ▸Table 1.2 provides an overview of the mandatory external interfaces of the TOE and provides additional information. Except for HAN-CON and HAN-CLS, all interfaces are separated both physically and logically.

Interface Name	Description
HAN-CLS	The TOE offers two physical interfaces HAN-CLS and HAN-CON to the HAN. All services of the TOE provided at HAN-CLS are also provided at HAN-CON and vice-versa. CLS may use the communication services of the TOE and the management functionality they have access to via these interfaces. The SRV has the possibility to use these interfaces to review information that is relevant to maintain the TOE and to use the management functionality they have access to. Via these interfaces, the TOE provides the consumer with the possibility to review information that is relevant for billing or concerns the privacy of the consumer. Specifically, the access to the consumer log is only allowed via these interfaces.
HAN-CON	
LMN	Interface between the meter and the TOE. In particular, the TOE receives meter data via this interface.
SM	The TOE invokes the services of its security module via this interface.
WAN	The TOE submits information to or receives information from authorized GWAs or external market participants via this interface. In particular, the GWA accesses the TOE only via this interface.

Table 1.2 Mandatory TOE external interfaces

Application Note 6: Please note that the interface to the security module is not considered as TSFI, since the physical representation of this interface shall be protected properly by the TOE casing itself. Nevertheless, the interface needs to be described by the developer in order to give the ITSEF the possibility to verify whether the security module is used in accordance with [SecMod-PP].

Application Note 7: Please note that in case the SMGW uses a communication adapter that is not part of the TOE, see ▸Section 1.4.5.2, all security-relevant functionality defined in ▸Chapter 6 has to be implemented within the TOE itself. This also holds true for TLS endpoints.

1.4.8 The cryptography of the TOE and its security module

Parts of the cryptographic functionality required for the functionality described in ▸Section 1.4.6 shall be provided by a security module. The security module provides strong cryptographic functionality, random number generation, secure storage of secrets and supports the authentication of the GWA. The security module is a different IT product and not part of the TOE as described in this PP. Nevertheless, it is physically embedded into the SMGW and protected by the same level of physical protection. The requirements for the security module are specified in [SecMod-PP].

The following table provides a more detailed overview on how the cryptographic functions are distributed between the TOE and its security module.

Aspect	TOE	Security module
Communication with external market participant	• encryption • decryption • hashing • key derivation • MAC generation • MAC verification • secure storage of TLS certificates	Support during TLS-handshake: • key agreement • secure storage of the private key of the TOE • digital signature verification for authentication of external entities • digital signature generation for authentication of the TOE • random number generation[15]
Communication with GWA		
Communication with consumer		
Communication with SRV		
Communication with CLS		
Communication with meter using TLS		
Unidirectional communication with meter	• encryption • decryption • key derivation • MAC generation • MAC verification • secure storage of the shared secret	-
Signing data before submission to an external entity	• hashing	• digital signature generation • secure storage of the private key of the TOE
Signature verification of data provided by an external entity	• hashing	• digital signature verification for authentication of external entities
Content data encryption and integrity protection	• encryption • key derivation • MAC generation • MAC verification • secure storage of the public key	• key agreement • secure storage of the private key of the TOE • random number generation
Wake-up message verification	• hashing	• digital signature verification
Key generation service	• key generation • certificate generation	• random number generation

Table 1.3 Cryptographic support of the TOE and its security module

Application Note 8: The security module may also store further keys such as the trust anchor of the smart metering PKI (for more details on the PKI see [BSI-TR-03109-4]). If the security module is used for such - and similar - purposes, the ST author shall add this information accordingly in ▸Table 1.3.

Application Note 9: It is not required that the TOE offers content data decryption. If it provides such cryptographic functionality, the ST author shall add this information accordingly in ▸Table 1.3.

The distribution of cryptographic functionality among the TOE and its security module has not only been decided from a security perspective but also considered aspects of performance. A significant part of the complex functionality is implemented by the TOE. A state-of-the-art security module in form of an integrated chip should be able to perform approximately ten connection establishments per minute. As the calculated session keys are valid for a longer period, this should be sufficient for most of the applications. In cases where this speed is not sufficient, the developer should consider alternative approaches, e.g., the use of multiple security modules.

[15] The RNG functionality or parts of it may also be provided by the TOE, see the application note in ▸Section 6.3.2.

1.4.8.1 Content data encryption vs. an encrypted channel

The TOE utilizes concepts of the encryption of data on the content level as well as the establishment of a trusted channel to external entities.

All communication with external entities is enforced to happen via encrypted, integrity protected and mutually authenticated channels.

Further, in the case that processed meter data are sent to an external market participant via the GWA, these data have to be protected on a content level using *CMS* (according to [BSI-TR-03109-1]).

The basic information flow for meter data is as follows:

1. The meter measures the consumption or production of a certain commodity.
2. The meter data is prepared for transmission:
   a. If the communication between the meter and the TOE is performed bidirectionally, the meter data is transmitted via an encrypted and mutually authenticated channel to the TOE. Please note that the submission of this information may be triggered by the meter or the TOE.
   b. If a unidirectional communication is performed between the meter and the TOE, the meter data is encrypted using a symmetric algorithm to ensure the authenticity and confidentiality.
3. The authenticity and integrity of the meter data is verified by the TOE.
4. If (and only if) authenticity and integrity have been verified successfully, the meter data is further processed by the TOE according to the rules in the processing profile, else the cryptographic information flow will be cancelled.
5. Depending on the processing profile, the processed meter data is signed using the services of the security module.
6. If the processed meter data are sent to a final recipient of the data via the GWA, processed meter data is additionally protected using CMS.
7. The processed meter data is submitted to an authorized external entity in the WAN via an encrypted and mutually authenticated channel. It may be sent to the external entity via the GWA.

1.4.9 TOE life cycle

The life cycle of the TOE can be separated into the following phases:

1. Development
2. Production
3. Pre-personalization at the developer's premises (without security module)
4. Pre-personalization and integration of security module
5. Delivery to the MPO
6. Delivery by the MPO to the installation and operational environment
7. Installation and start of operation
8. Personalization
9. Normal operation
10. De-installation

For a detailed description of the life cycle phases, see [BSI-TR-03109-1-VIII].

For the PP, it is important to know that the certified configuration of the TOE will be established after phase “personalization”. It has to be ensured that previous phases are performed by trusted personnel in secure environments. Since the realization of the phases depends on the specific TOE, it is important that the TOE developer considers and enforces appropriate security measures during the life cycle phases. The TOE life cycle will be examined during evaluation of assurance aspect ALC.

Note that after reception of the TOE by the metering point operator (MPO), the MPO is responsible for the secure delivery of the TOE to the installation and operational environment. A de-installation of the TOE not only prior to decommission, but also to re-install it at another location is permitted, that is, a repetition of phases 6-10 (excluding phase 8 as the TOE is already personalized) is permitted. For the delivery to the location of re-installation, possibly with storage of the TOE in the MPO's premises, the same requirements as for the first delivery have to be met. Prior to a de-installation of a TOE, the user data present on the TOE have to be removed or made inaccessible. Therefore, the GWA or SRV have to make use of the user data reset functionality of the TOE beforehand.

2 Conformance Claims

2.1 Conformance statement

This PP requires strict conformance of any PP/ST to this PP.

2.2 CC Conformance Claims

This PP has been developed using Revision 1 of CC:2022 [CC:2022].

This PP is [CC:2022] Part 2 extended due to the use of FPR_CON.1.

This PP claims conformance to [CC:2022] Part 3; no extended assurance components have been defined.

2.3 PP Claim

This PP does not claim conformance to any other PP.

2.4 Conformance claim rationale

Since this PP does not claim conformance to any PP, this section is not applicable.

2.5 Package Claim

This PP claims an assurance package EAL4 augmented by AVA_VAN.5 and ALC_FLR.2 as defined in [CC:2022] Part 5 for product certification.

3 Security problem definition

3.1 External entities

The following external entities interact with the TOE. Those roles have been defined for the use in this PP. It is possible that a party implements more than one role in practice. For each external entity and each role they assume, a separate user identity is required to distinguish between them, see also ▸FIA_ATD.1.

Role	Description
Consumer (CON)	The authorized natural person or legal entity the meter data are associated with. In most cases, this will be tenants or house owners consuming electricity, water, gas or further commodities. However, it is also possible that the consumer produces or stores energy (e.g., with their own solar plant). The term consumer may be used as for the person as for consumer-owned devices that gain access to user data e.g. for visualization. The consumer may interact with the TOE at the HAN-CON or HAN-CLS interface. Communication profiles for consumers are configured in the TOE by the GWA.
Gateway administrator (GWA)	Authority that configures, monitors, and controls the TOE via the WAN interface.
Service technician (SRV)	The authorized individual that may interact with the TOE at its HAN-CON or HAN-CLS interface for diagnostic and maintenance purposes. The term SRV may be used for the person or for the communication device they use. In terms of managing the TOE, the SRV can be considered as the local extension of the GWA and therefore has a limited access to management functionality. In terms of the delivery procedures of the TOE, the SRV can be considered as an entity authorized by the MPO.
External market participant	External entity configured by the GWA with corresponding profiles in the TOE and connected via WAN that might receive meter data or controls CLS devices connected to the TOE.
Meter	Device that is connected to the TOE via the LMN interface to measure and report meter data. Hypernym for residential and industrial meters in the LMN. Communication profiles for meters are configured in the TOE by the GWA.
CLS	External entity that is connected to the TOE via the HAN-CON or HAN-CLS interface and that uses the TOE for dedicated communication purposes. Communication profiles for CLS are configured in the TOE by the GWA.
Metering point operator (MPO)	In the context of this PP, the entity that is responsible for parts of the delivery and for the installation of the TOE.
External entity	Human or IT entity possibly interacting with the TOE from outside of the TOE boundary. In the context of this PP, the terms user or external entity serve as a hypernym for all entities mentioned before.

Table 3.1 Roles used in this PP

3.2 Assets

The following table introduces the relevant assets for this protection profile and their need for protection. Note that this table does not address the permitted access of external entities to these assets.

The table focuses on the assets that are relevant for the TOE and does not claim to provide an overview over all assets in the smart metering system or for other devices in the LMN.

Asset	Description	Need for protection	user/TSF data
Meter data	Meter readings that allow calculation of the quantity of a commodity, e.g., electricity, gas, water or heat consumed over a period. This includes already time-stamped meter values as well as load time series of meters. The data of industrial meters in the HAN sent to the TOE are not considered meter data.	• Integrity and authenticity • Confidentiality	user data

Asset	Description	Need for protection	user/TSF data
System log data	Log data from the system log.	• Integrity • Confidentiality	TSF data
Consumer log data	Log data from the consumer log.	• Integrity • Confidentiality	user data
Calibration log data	Log data from the calibration log.	• Integrity • Confidentiality	TSF data
Supplementary data	The TOE may be used for communication purposes by devices in the LMN or HAN. It may be that the functionality of the TOE that is used by such a device is limited to pure (but secure) communication services. Data that is transmitted via the TOE but that does not belong to one of the aforementioned data types is named supplementary data.	• According to their specific need	user data
Data	The term data is used as a hypernym for meter data and supplementary data.	• According to their specific need	user data
SMGW time	Date and time of the real-time clock of the TOE. SMGW time is e.g. used in meter data records sent to external market participants.	• Integrity • Authenticity (when time is adjusted to an external reference time)	TSF data
Personally identifiable information (PII)	Personally identifiable information refers to information that can be used to uniquely identify, contact, or locate a natural person or can be used with other sources to uniquely identify a single individual.	• Confidentiality	user data
CLS config	Configuration data of a CLS, such as software updates.	• Integrity and authenticity • Confidentiality	user data
Meter config	Configuration data of a meter, such as software updates.	• Integrity and authenticity • Confidentiality	user data
HAN device key pair	Contains the private-public key pair data generated by the TOE for the asymmetric cryptographic functionality of the device in the HAN. Optionally also contains the corresponding self-signed certificate.	• Integrity and authenticity • Confidentiality (only for the private key)	user data
Meter key pair	Contains the private-public key pair data generated by the TOE for the meter's asymmetric cryptographic functionality. Optionally also contains the corresponding self-signed certificate.	• Integrity and authenticity • Confidentiality (only for the private key)	user data
Meter symmetric key	Symmetric key for unidirectional communication with meters in the LMN.	• Integrity and authenticity • Confidentiality	TSF data
Memory encryption key	Symmetric key used by the TOE to secure its persistent memory.	• Integrity and authenticity • Confidentiality	TSF data
Processing profile	A processing profile determines which data shall be sent to which external entity and by whom the data may be accessed.	• Integrity and authenticity • Confidentiality	TSF data
Tarifing event data	Data for event-based processing profiles that invoke the capture of meter data based on an internal or external event.	• Integrity and authenticity	TSF data

Asset	Description	Need for protection	user/TSF data
Communication profile	Set of data containing parameters necessary for communication with an external entity. Includes certificates of the external entity but not the certificates/key material of the TOE.	• Integrity and authenticity	TSF data
Certificates	Certificates of the TOE.	• Integrity and authenticity	TSF data
Firmware update	Firmware update that is downloaded by the TOE to update the firmware of the TOE.	• Integrity and authenticity	TSF data
Ephemeral keys	Ephemeral cryptographic material used by the TOE for cryptographic operations.	• Integrity and authenticity • Confidentiality (except for public keys)	TSF data
Consumer password hash	Hash of the consumer password	• Integrity and authenticity • Confidentiality	user data

Table 3.2 Assets

3.3 Assumptions

In this threat model, the following assumptions about the environment of the components need to be taken into account in order to ensure a secure operation.

A.ExternalPrivacy It is assumed that authorized and authenticated external entities receiving any kind of privacy-relevant data or billing-relevant data and the applications that they operate are trustworthy (in the context of the data that they receive) and do not perform unauthorized analyses of this data with respect to the corresponding consumer(s).

A.TrustedAdmins It is assumed that the GWA and the SRV are trustworthy and well-trained.

It is assumed that the GWA or the SRV use the user data reset functionality of the TOE prior to a de- and subsequent re-installation of the TOE.

If the GWA or the SRV delete calibration log data (except for events logging successful firmware updates) in context of a user data reset, it is assumed that they export the data beforehand and store them outside the TOE to ensure the required availability of said data.

A.PhysicalProtection It is assumed that the TOE and all connected meters are installed at the same grid connection point,

- either in a non-public environment within a closed facility with restricted access[16], which provides a basic level of physical protection. The level of physical protection that is expected to be provided by the environment is the same level of protection that is expected for classical meters that operate according to the regulations of the national calibration authority. This protection covers the TOE, the meter(s) that the TOE communicates with, devices in the HAN as well as the communication channel between the TOE and its security module,
- or in a public environment within a concealing casing[17] which provides a basic level of physical protection for the TOE, including the restriction of direct access to the TOE and mechanisms to detect manipulation. This protection covers the TOE, the meters that the TOE communicates with, devices in the HAN as well as the communication channel between the TOE and its security module.

[16] This may also comprise the premises of the MPO.

[17] For example distribution cabinets.

If the TOE is not installed within a closed facility but within a public environment, i.e., the latter case, then it is assumed that the asset PII is neither present on the TOE nor transmitted via the TOE.

A.ExtensionLocalNetwork It is assumed that the spatial expansion of the networks HAN and LMN is restricted to the premises of the consumer.

A.Profile The processing profiles and communication profiles that are used when handling data are assumed to be trustworthy and correct.

Application Note 10: The processing profiles, which are used for information flow control, are an essential factor for the preservation of the privacy of the consumer. The processing profiles are used to determine which data shall be sent to which entity at which frequency and how data are processed. For example, they determine whether the data needs to be related to the consumer (for billing purposes) or whether the data shall be pseudonymized.

The processing profiles shall be visible for the consumer to allow a transparent communication.

It is essential that processing profiles correctly define the amount of information that must be sent to an external market participant. Exact regulations regarding the processing profiles and the GWA are beyond the scope of this PP. Nevertheless, only those processing profiles are permitted which are realized according to [BSI-TR-03109-1] or which are defined in accompanying documents to [BSI-TR-03109-1]. Further processing profiles are not permitted and shall not be accepted by the TOE.

A.Update It is assumed that firmware updates for the TOE that can be provided by an authorized external entity have undergone a certification process according to this PP before they are issued and can therefore be assumed to be correctly implemented. It is further assumed that the external entity that is authorized to provide the firmware update is trustworthy and will not introduce any malware into a firmware update.

A.Network It is assumed that

1. a WAN network connection with a sufficient reliability and bandwidth for the individual situation is available,
2. one or more trustworthy sources for an update of the SMGW time are available in the WAN,
3. residential meters in the LMN communicate exclusively with the TOE and only the TOE is able to decrypt the data sent by the residential meter,
4. industrial meters in the LMN connected to the TOE only have additional unidirectional (outbound) connections to other networks,
5. if devices in the HAN have a separate connection (beside the TOE) to parties in other networks, this connection is appropriately protected,
6. devices connected to the TOE do not provide any kind of network connection between HAN, LMN and WAN, and
7. all wired connections are connected properly to prevent non-reachability of the TOE due to false-connections of WAN and HAN interfaces.

Note that a certification according to [BSI-TR-03109-5] for devices in the scope of said technical guideline is sufficient for point 5 of this assumption to hold.

Application Note 11: The assumption for the connection between a TOE and connected meters in the LMN holds on a logical level rather than on a physical one. It may be possible, that the meters in the LMN have a physical connection to other devices that would in theory also allow a communication, e.g. when wireless communication technologies are used. It is further possible that signals of meters are amplified by other devices or other meters on the physical layer without violating this assumption. However, it is assumed that the the meters do only communicate with the TOE and that only the TOE is able to decrypt the data sent by the meter.

A.Keygen It is assumed that the shared, meter-individual keys for the communication with meters are generated securely according to [BSI-TR-03109-3] and brought into the TOE in a secure way by the GWA.

A.Delivery After the reception of the TOE by the MPO, the MPO is responsible for the secure delivery of the TOE to the installation and operational environment. It is assumed that the MPO is trustworthy in context of this delivery and well trained and takes appropriate security measures to ensure protection against undetected manipulation or undetected replacement of the TOE during such a delivery to ensure integrity and authenticity of the TOE.

This also holds in the case of a de-installation and then re-installation of the TOE at another location.

Note that adhering to [MSB-LK] is sufficient for MPOs to fulfill this assumption.

A.IndustrialMeterHAN It is assumed that if an industrial meter is connected to the TOE via the HAN, then the industrial meter is the end point of the TLS proxy functionality provided by the TOE.

3.4 Threats

The following sections identify the threats that are posed against the assets handled by the TOE of smart metering systems. Those threats are the result of a threat model that has been developed for the whole smart metering system first and then has been focused on the threats against the TOE.

It should be noted that the threats in the following paragraphs consider two different kinds of attackers:

- *Local attacker*: An attacker that has
  - physical access to meter, TOE, a connection between these components, or
  - local logical access, including access to wireless connections, to any of the interfaces,

  who tries to disclose or alter assets while stored in the TOE or while transmitted between external entities and the TOE.

  Considering the limited value of information processed by a single TOE (resulting in a lower attack motivation in comparison to remote attacks on a large number of TOEs), the necessity for easy access to the consumer's data and the basic physical protection of the consumer premises (cf. A.PhysicalProtection), the following threat model assumes for the vulnerability assessment, that local attackers have laymen expertise and use standard equipment only. However, the preparation of local attacks in terms of developing the attack path incl. tools can be performed by attackers with full AVA_VAN.5 attack potential (e.g., expert expertise), as long as their execution is possible with the restrictions for local attackers mentioned above.

  Additionally, all drilling, cutting and milling attacks to permanently visible surfaces of the physical device (which can be inspected by consumers and/or SRVs) can be neglected in the considerations of identifying attack paths during AVA_VAN, since attacks to the TOE case are supposed to be detected during an inspection. Therefore, the application of any kind of stickers to the TOE case is forbidden, except the seal for the casing acc. to ▸FPT_PHP.1. All surfaces, which are not visible permanently, on the other hand, shall be evaluated during AVA aspects for potential vulnerabilities (e.g. non-bypassibility).

  Please note that the local attacker includes authorized entities like consumers.

- *Remote attacker*: An attacker that is located in the WAN and who tries to compromise the confidentiality, authenticity and/or integrity of the processed meter data and or configuration data transmitted via the WAN, or who tries to conquer a component of the infrastructure (i.e., meter, TOE or CLS) via the WAN to cause damage to a component itself or to the corresponding grid (e.g., by sending forged meter data to an external market participant).

  Please note that the remote attacker includes entities like external market participants.

The specific rationale for this situation is given by the expected benefit of a successful attack. An attacker who needs physical access to the TOE that they are attacking will only be able to compromise one TOE at a time. Thus, the effect of a successful attack will always be limited to the attacked TOE. An attack from the WAN side on the other hand may potentially compromise a large number of TOEs.

T.DataModificationLocal A local attacker may try to modify (i.e., alter, insert, replay or redirect) user data (e.g., meter data, CLS config) or TSF data when transmitted between the TOE and external entities. The attacker may perform the attack via any interface (LMN, HAN, or WAN).

When trying to modify meter data, it is the objective of the local attacker to alter billing-relevant information or grid status information.

When trying to modify the CLS config or meter config, it is the objective of the local attacker to influence the behavior of CLS or meters.

In order to achieve the modification, the attacker may also try to modify TSF data such as the firmware of the TOE.

T.DataModificationWAN A remote attacker may try to modify (i.e. alter, insert, replay or redirect) user data (e.g., meter data, CLS config) or TSF data (e.g. firmware update) when transmitted between the TOE and an external entity in the WAN.

When trying to modify meter data, it is the objective of the remote attacker to modify billing-relevant information or grid status information.

When trying to modify the CLS config or meter config, it is the objective of the remote attacker to influence the behavior of CLS or meters.

When trying to modify TSF data such as a firmware update, the remote attacker tries to circumvent security mechanisms of the TOE or tries to get control over the TOE or a device in the HAN or LMN via the TOE.

T.TimeModification A local attacker or remote attacker may try to alter the SMGW time on the TOE, during the transmission between the external time source and the TOE or during the transmission between the TOE and external entities in the HAN.

The motivation of the attacker could be for example to change the relation between date/time and measured consumption or production values in the meter data records (e.g. to influence the balance of the next invoice).

T.DisclosureWAN A remote attacker may try to read/disclose confidential information in the user data, e.g., meter data or the CLS config, when transmitted between TOE and external entities in the WAN.

T.DisclosureLocal A local attacker may try to read/disclose confidential information in the user data, e.g., the CLS config, HAN device key pairs or meter key pairs, when transmitted between the TOE and external entities.

T.Infrastructure A remote attacker may try to obtain control over the TOE or over devices in the HAN or LMN via the TOE to cause damage to external entities, for example by altering user data or TSF data.

A remote attacker may also try to conquer a CLS in the HAN first in order to remotely attack the TOE from the HAN side.

T.ResidualData A local attacker or a remote attacker may try to read/disclose user data (e.g., meter data) from the TOE which are no longer needed by the TOE.

T.ResidentData A remote attacker or local attacker may try to access (i.e., read, alter, delete) user data or TSF data which they don't have permission to while the information is stored in the TOE.

While the remote attacker only uses the WAN interface of the TOE, the local attacker may also physically access the TOE.

T.Privacy A remote attacker may try to obtain more detailed information from the TOE than actually required to fulfil the tasks defined by its role or the contract with the consumer. This includes scenarios in which an external market participant that is primarily authorized to obtain certain information from the TOE, tries to obtain more information permitted, as well as scenarios in which an attacker who is not authorized at all tries to obtain information.

3.5 Organizational Security Policies (OSPs)

This section lists the organizational security policies (OSP) that the TOE shall comply with:

OSP.SM

The TOE shall use the services of a certified security module for

1. generation of digital signatures,
2. verification of digital signatures,
3. key agreement for TLS and for content data encryption,
4. key pair generation,
5. random number generation,
6. component authentication via the PACE protocol with negotiation of session keys,
7. secure messaging between TOE and security module, and
8. secure storage of key material for the TOE.

The security module shall be certified according to [SecMod-PP] and shall be used in accordance with its relevant guidance documentation. In particular, the certificate of the security module shall be valid when the TOE is delivered to the operational environment.

OSP.Log

The TOE shall maintain a set of log files as defined in [BSI-TR-03109-1] as follows:

1. A system log of relevant events in order to allow an authorized GWA to analyze the status of the TOE. The TOE shall also analyze the system log automatically for a cumulation of security relevant events.
2. A consumer log that contains information about the information flows that have been initiated to the WAN and information about the processing profiles causing this information flow as well as the billing-relevant information.
3. A calibration log (as defined in ▸Section 6.2.1) that provides the GWA with a possibility to review calibration relevant events.

The TOE shall further limit access to the information in the different log files as follows:

1. Access to the information in the system log shall only be allowed for an authorized GWA via WAN and an authorized service technician via HAN-CLS or HAN-CON.
2. Access to the information in the calibration log shall only be allowed for an authorized GWA via WAN and an authorized service technician via HAN-CLS or HAN-CON.
3. Access to the information in the consumer log shall only be allowed for an authorized consumer via HAN-CLS or HAN-CON. The consumer shall only have access to their own information.

The system log may overwrite the oldest events in case that the audit trail gets full.

For the consumer log, the TOE shall ensure that a sufficient number of events is available (in order to allow a consumer to verify an invoice) but may overwrite events older than 15 months in case that the audit trail gets full.

For the calibration log, the following rules apply: Events shall be available for three years counting from the end of the year of generation of said events according to national regulations. To ensure this availability, most events may be stored outside the TOE, e.g. if an export of the calibration log data is necessary prior to a TOE reset due to a de-installation of the TOE or if the calibration log storage is full. An exeption are certain events listed in [BSI-TR-03109-1], such as events on successful firmware updates, that shall be available on the TOE.

OSP.KeyGenService The TOE shall provide the following key generation services for the respective external entities:

1. the generation of private-public key pairs and corresponding self-signed certificates for CLS in the HAN and meters in the LMN
2. the generation of *pre-shared keys* for meters in the LMN

4 Security Objectives

4.1 Security objectives for the TOE

O.Firewall

The TOE shall serve as the connection point for external entities and shall provide firewall functionality in order to protect the devices of the LMN and HAN (as long as they use the TOE) and itself against threats from the WAN side.

The firewall:

1. shall not allow any connections between the WAN and LMN, WAN and HAN, LMN and HAN,
2. shall allow connections to devices in the WAN established by the TOE,
3. shall allow connections to devices in the LMN established by the TOE or by the meter,
4. shall allow connections to consumers established by the consumer,
5. shall allow connections to CLS established by the TOE or by the CLS,
6. shall allow connections to SRVs established by the SRV,
7. shall provide a wake-up service on the WAN interface to trigger the allowed connection establishments with external entities in the WAN,
8. shall not allow any other services being offered on the WAN interface,
9. shall allow connections between external entities in the WAN and CLS via the TOE established by the TOE or the CLS,
10. shall allow communication flows only if confidentiality-protected and integrity-protected and if endpoints are authenticated.

O.SeparateIF

The TOE shall have physically separated ports for the WAN, the LMN, the HAN-CON and the HAN-CLS interface.

O.ConcealWAN

To protect the privacy of its consumers, the TOE shall conceal the communication with external entities in the WAN in order to ensure that no privacy-relevant information may be obtained by analyzing the frequency, load, size or the absence of external communication.

O.Meter

The TOE receives or polls information about the consumption or production of different commodities from one or multiple meters in the LMN and is responsible for handling meter data. This includes that:

1. the TOE shall ensure that the communication to the meter(s) in the LMN is established in an GWA-definable interval, or an interval as defined by the meter, or on demand of the TOE,
2. the TOE shall enforce encryption and integrity protection for the communication with the meter,
3. the TOE shall verify the integrity and authenticity of the data received from a meter before handling it further,
4. the TOE shall process the data according to the definition in the corresponding processing profile,
5. the TOE shall encrypt the processed meter data for the final recipient if they are sent via a third party and
6. deliver the encrypted data to authorized external market participants as defined in the corresponding processing profiles facilitating an encrypted channel,
7. if an external market participant cannot be reached, the TOE shall re-try to send the data until a configurable number of unsuccessful retries has been reached,
8. the TOE shall pseudonymize the data for parties that do not need the relation between the processed meter data and the identity of the consumer according to the corresponding processing profiles managed by the GWA only.

O.Crypt

The TOE shall provide cryptographic functionality as follows:

1. authentication, integrity protection and encryption of the communication and data to external entities in the WAN,
2. authentication, integrity protection and encryption of the communication to the meter,
3. authentication, integrity protection and encryption of the communication to the consumer, SRV and CLS,
4. authentication, integrity protection and encryption of the communication for CLS to WAN and/or WAN to CLS connections,
5. replay detection for all communications with external entities,
6. encryption of the persistently stored TSF and user data of the TOE, and
7. generation of a public-private-key pair and a corresponding self-signed certificate for CLS and meters.

In addition, the TOE shall generate the required keys utilizing the services of its security module[18] and ensure that the keys are only used for an acceptable amount of time. Further, the TOE shall destroy ephemeral keys if no longer needed, as well as the private keys generated for CLS and meters after deployment.

O.Time

The TOE shall provide reliable time stamps and update its internal clock in regular intervals by retrieving reliable time information from a dedicated reliable source in the WAN.

O.Protect

The TOE shall implement functionality to protect its security functions against malfunctions and tampering. Specifically, the TOE shall

[18] Please refer to chapter ▸Section 1.4.8 for an overview on how the cryptographic functions are distributed between the TOE and its security module.

1. encrypt its TSF and user data as long as it is not in use,
2. overwrite any information that is no longer needed to ensure that it is no longer available via the external interfaces of the TOE,
3. monitor user data and the TSF for integrity errors,
4. have a fail-safe design ensuring that it preserves a *secure state* when a malfunction occurs, and
5. make any physical manipulation within the scope of the intended environment detectable for the consumer or SRV.

O.Management The TOE shall only provide authorized GWAs with functions for the management of the security features, with exceptions as follows. The following limited functions for the management of the security features are available to the respective external entities when authorized:

- The authorized SRV may manage WAN communication parameters as well as initiate a self-test, a restart or a reset of the TOE via HAN-CON or HAN-CLS.
- The authorized consumer may change their own password via HAN-CON or HAN-CLS.
- The authorized CLS may initiate the establishment of a communication channel with an external market participant.

Further, the TOE shall implement a secure mechanism to update the firmware of the TOE that ensures that only authorized entities are able to provide updates for the TOE and that only authentic and integrity protected updates are applied.

O.Log The TOE shall maintain a set of log files as defined in [BSI-TR-03109-1] for each external GWA, consumer and/or SRV defined in the TOE and its processing profiles as follows:

1. A system log of relevant events in order to allow an authorized GWA or an authorized SRV to analyze the status of the TOE. The TOE shall also analyze the system log automatically for a cumulation of security relevant events.
2. A consumer log that contains information about the information flows that have been initiated to the WAN and information about the processing profiles causing these information flows as well as information about the system status (including relevant error messages).
3. A calibration log that provides the GWA and the SRV with a possibility to review calibration relevant events.

The TOE shall further limit access to the information in the different log files as follows:

1. Access to the information in the system log shall only be allowed for an authorized GWA via WAN or for an authorized SRV via HAN-CON or HAN-CLS.
2. Access to the information in the consumer log shall only be allowed for an authorized consumer via the HAN-CON or HAN-CLS interface of the TOE and via a secured (i.e., confidentiality and integrity protected) connection. The consumer shall only have access to their own information.
3. Access to the information in the calibration log shall only be allowed for an authorized GWA via the WAN interface and for an authorized SRV via the HAN-CON or HAN-CLS interface of the TOE.

The system log may overwrite the oldest events in case that the audit trail gets full.

For the consumer log, the TOE shall ensure that a sufficient number of events is available (in order to allow a consumer to verify an invoice) but may overwrite events older than 15 months in case that the audit trail gets full.

If the audit trail of the calibration log gets full, the TOE shall reversibly stop operation, ignore audited events and inform the GWA. The TOE shall allow for a deletion of the data by the GWA and SRV except for events required to remain according to [BSI-TR-03109-1].

O.Access The TOE shall control the access of external entities in WAN, HAN or LMN to any information that is sent to, from or via the TOE via its external interfaces. Only the SMGW time may be accessed by external entities in HAN and LMN without prior authentication.

O.KeyGenService The TOE shall provide the following key generation services for the respective external entities:

1. the generation of private-public key pairs and corresponding certificates for CLS in the HAN and meters in the LMN and
2. the generation of pre-shared keys for meters in the LMN.

The authorized CLS or authorized meter may request the generation and delivery of a public-private-key pair and the corresponding self-signed certificate.

4.2 Security objectives for the operational environment

OE.ExternalPrivacy Authorized and authenticated external entities receiving any kind of private or billing-relevant data shall be trustworthy and shall not perform unauthorized analyses of these data with respect to the corresponding consumer(s).

OE.TrustedAdmins The GWA and the SRV shall be trustworthy and well-trained.

The GWA and the SRV shall use the user data reset functionality of the TOE prior to a de- and subsequent re-installation of the TOE.

If the GWA or the SRV delete calibration log data (except for events logging successful firmware updates) in context of a user data reset, it is assumed that they export the data beforehand and store them outside the TOE to ensure the required availability of said data.

OE.PhysicalProtection The TOE and all connected meters shall be installed at the same grid connection point,

- in a non-public environment within a closed facility with restricted access that provides a basic level of physical protection. This protection shall cover the TOE, the meters that the TOE communicates with, devices in the HAN as well as the communication channel between the TOE and its security module. Only authorized individuals may physically access the TOE.
- or in a public environment within a concealing casing which provides a basic level of physical protection for the TOE, including the restriction of direct access to the TOE and mechanisms to detect manipulation. This protection shall cover the TOE, the meters that the TOE communicates with, devices in the HAN as well as the communication channel between the TOE and its security module. Only authorized individuals may physically access the TOE.

If the TOE is not installed within a closed facility but within a public environment, i.e., the latter case, then the asset PII shall neither be present on the TOE nor transmitted via the TOE.

OE.ExtensionLocalNetwork The spatial expansion of the networks HAN and LMN shall be restricted to the premises of the consumer.

OE.Profile The processing profiles and communication profiles that are used when handling data shall be obtained from a trustworthy and reliable source only.

OE.SM The environment shall provide the services of a certified security module for:

1. verification of digital signatures,
2. generation of digital signatures,
3. key agreement,
4. key transport,
5. key storage, and
6. random number generation.

The security module used shall be certified according to [SecMod-PP] and shall be used in accordance with its relevant guidance documentation. In particular, the certificate of the security module shall be valid when the TOE is delivered to the operational environment.

OE.Update The firmware updates for the TOE that can be provided by an authorized external entity shall undergo a certification process according to this PP before they are issued to show that the update is implemented correctly. The external entity that is authorized to provide the update shall be trustworthy and ensure that no malware is introduced via a firmware update.

OE.Network It shall be ensured that

1. a WAN network connection with a sufficient reliability and bandwidth for the individual situation is available,
2. one or more trustworthy sources for an update of the system time are available in the WAN,
3. residential meters in the LMN do communicate exclusively with the TOE and only the TOE is able to decrypt the data sent by the residential meter,
4. industrial meters in the LMN connected to the TOE only have additional unidirectional (outbound) connections to other networks,
5. if devices in the HAN have a separate connection (beside the TOE) to parties in other networks, this connection is appropriately protected,
6. devices connected to the TOE do not provide any kind of network connection between HAN, LMN and WAN, and
7. all wired connections are connected properly to ensure the correct operation.

Note that a certification according to [BSI-TR-03109-5] for devices in the scope of said technical guideline is sufficient for point 5 of this security objective to be satisfied.

Application Note 12: The security objective for the connection between a TOE and connected meters in the LMN holds on a logical level rather than on a physical one. It may be possible, that the meters in the LMN have a physical connection to other devices that would in theory also allow a communication, e.g. when wireless communication technologies are used. It is further possible that signals of meters are amplified by other devices or other meters on the physical layer without violating this assumption. However, the meters shall only communicate with the TOE and only the TOE shall be able to decrypt the data sent by the meter.

OE.Keygen It shall be ensured that the shared, meter-individual keys for the communication with meters are generated securely according to [BSI-TR-03109-3] and brought into the TOE in a secure way by the GWA.

OE.Delivery After the reception of the TOE by the MPO, the MPO is responsible for the secure delivery of the TOE to the installation and operational environment. The MPO shall be trustworthy in context of this delivery and well trained and shall take appropriate security measures to ensure protection against undetected manipulation or undetected replacement of the TOE during such a delivery to ensure integrity and authenticity of the TOE.

This also holds in the case of a de-installation and then re-installation of the TOE at another location.

Note that adhering to [MSB-LK] is sufficient for MPOs to fulfill this security objective.

OE.IndustrialMeterHAN It shall be ensured that if an industrial meter is connected to the TOE via the HAN, then the industrial meter is the end point of the TLS proxy functionality provided by the TOE.

4.3 Security objectives rationale

4.3.1 Overview

▸Table 4.1 gives an overview how the assumptions, threats, and organizational security policies are addressed by the security objectives. The text of the following sections justifies this more in detail.

	O.Firewall	O.SeparateIF	O.ConcealWAN	O.Meter	O.Crypt	O.Time	O.Protect	O.Management	O.Log	O.Access	O.KeyGenService	OE.SM	OE.ExternalPrivacy	OE.TrustedAdmins	OE.PhysicalProtection	OE.ExtensionLocalNetwork	OE.Profile	OE.Update	OE.Network	OE.Keygen	OE.Delivery	OE.IndustrialMeterHAN
T.DataModificationLocal				X	X		X	X						X	X							
T.DataModificationWAN	X				X		X	X						X								
T.TimeModification					X	X	X	X						X	X							
T.DisclosureWAN	X		X		X		X	X						X								
T.DisclosureLocal				X	X		X	X						X	X							
T.Infrastructure	X	X		X	X		X	X						X								
T.ResidualData							X	X						X								
T.ResidentData	X				X		X	X		X				X	X							
T.Privacy	X		X	X	X		X	X		X				X			X					
OSP.SM					X		X	X				X		X								
OSP.Log							X	X	X	X				X								

	O.Firewall	O.SeparateIF	O.ConcealWAN	O.Meter	O.Crypt	O.Time	O.Protect	O.Management	O.Log	O.Access	O.KeyGenService	OE.SM	OE.ExternalPrivacy	OE.TrustedAdmins	OE.PhysicalProtection	OE.ExtensionLocalNetwork	OE.Profile	OE.Update	OE.Network	OE.Keygen	OE.Delivery	OE.IndustrialMeterHAN
OSP.KeyGenService					X		X	X		X	X			X								
A.ExternalPrivacy													X									
A.TrustedAdmins														X								
A.PhysicalProtection															X							
A.ExtensionLocalNetwork																X						
A.Profile																	X					
A.Update																		X				
A.Network																			X			
A.Keygen																				X		
A.Delivery																					X	
A.IndustrialMeterHAN																						X

Table 4.1 Rationale for security objectives

4.3.2 Countering the threats

The following sections provide more detailed information on how the threats are countered by the security objectives for the TOE and its operational environment.

4.3.2.1 General objectives

The security objectives O.Protect, O.Management and OE.TrustedAdmins contribute to counter each threat and contribute to each OSP.

O.Management is indispensable as it defines the requirements around the management of the Security Functions. Without a secure management no TOE can be secure. Also **OE.TrustedAdmins** contributes to this aspect as it provides the requirements on the availability of a trustworthy GWA and SRV. **O.Protect** is present to ensure that all security functions are working as specified.

Those general objectives will not be addressed in detail in the following paragraphs.

4.3.2.2 T.DataModificationLocal

The threat **T.DataModificationLocal** is countered by a combination of the security objectives **O.Meter**, **O.Crypt** and **OE.PhysicalProtection.**

O.Meter defines that the TOE will enforce the encryption of communication when receiving meter data from the meter. **O.Crypt** defines the required cryptographic functionality. The encryption of the persistent memory according to O.Crypt supports the protection of the TOE against local attacks. The objectives together ensure that the communication between the TOE and external entities cannot be modified or released.

OE.PhysicalProtection is of relevance as it ensures that access to the TOE is limited.

4.3.2.3 T.DataModificationWAN

The threat **T.DataModificationWAN** is countered by a combination of the security objectives **O.Firewall** and **O.Crypt**.

O.Firewall defines the connections for the devices within the LMN and HAN to external entities within the WAN and shall provide firewall functionality in order to protect the devices of the LMN and HAN (as long as they use the TOE) and itself against threats from the WAN side. **O.Crypt** defines the required cryptographic functionality. Both objectives together ensure that the data transmitted between the TOE and the WAN cannot be modified by a remote attacker.

4.3.2.4 T.TimeModification

The threat **T.TimeModification** is countered by a combination of the security objectives **O.Time, O.Crypt** and **OE.PhysicalProtection**.

O.Time defines that the TOE needs a reliable time stamp mechanism that is also updated from reliable sources regularly in the WAN. **O.Crypt** defines the required cryptographic functionality for the communication to external entities. Therewith, **O.Time** and **O.Crypt** are the core objective to counter the threat **T.TimeModification**.

OE.PhysicalProtection is of relevance as it ensures that access to the TOE is limited.

4.3.2.5 T.DisclosureWAN

The threat **T.DisclosureWAN** is countered by a combination of the security objectives **O.Firewall**. **O.ConcealWAN** and **O.Crypt**.

O.Firewall defines the connections for the devices within the LMN and HAN to external entities within the WAN and shall provide firewall functionality in order to protect the devices of the LMN and HAN (as long as they use the TOE) and itself against threats from the WAN side. **O.Crypt** defines the required cryptographic functionality. Both objectives together ensure that the communication between the meter and the TOE cannot be disclosed.

O.ConcealWAN ensures that no information can be disclosed based on additional characteristics of the communication like frequency, load or the absence of a communication.

4.3.2.6 T.DisclosureLocal

The threat **T.DisclosureLocal** is countered by a combination of the security objectives **O.Meter**, **O.Crypt** and **OE.PhysicalProtection**.

O.Meter defines that the TOE will enforce the encryption and integrity protection of communication when polling or receiving meter data from the meter. **O.Crypt** defines the required cryptographic functionality.The encryption of the persistent memory according to O.Crypt supports the protection of the TOE against local attacks. Both objectives together ensure that the communication between the TOE and external entities cannot be disclosed.

OE.PhysicalProtection is of relevance as it ensures that access to the TOE is limited.

4.3.2.7 T.Infrastructure

The threat **T.Infrastructure** is countered by a combination of the security objectives **O.Firewall**, **O.SeparateIF**, **O.Meter** and **O.Crypt**.

O.Firewall is the core objective that counters this threat. It ensures that all communication flows to the WAN are initiated by the TOE. The fact that the TOE does not offer any services to the WAN side and will not react to any requests (except the wake-up call) from the WAN is a significant aspect in countering this threat. Further the TOE will only communicate using encrypted channels to authenticated and trustworthy parties which mitigates the possibility that an attacker could try to hijack a communication.

O.Meter defines that the TOE will enforce the encryption and integrity protection for the communication with the meter.

O.SeparateIF facilitates the disjunction of the WAN from the LMN.

O.Crypt supports the mitigation of this threat by providing the required cryptographic primitives.

4.3.2.8 T.ResidualData

The threat **T.ResidualData** is mitigated by the security objective **O.Protect** as this security objective defines that the TOE shall delete information as soon as it is no longer used. Assuming that a TOE follows this requirement, an attacker cannot read out any residual information as it does simply not exist.

4.3.2.9 T.ResidentData

The threat **T.ResidentData** is countered by a combination of the security objectives **O.Access**, **O.Firewall, O.Protect** and **O.Crypt**. Further, the environment (**OE.PhysicalProtection** and **OE.TrustedAdmins**) contributes to this.

O.Access defines that the TOE shall control the access of users to information via the external interfaces.

The aspect of a local attacker with physical access to the TOE is covered by a combination of **O.Protect** (defining the detection of physical manipulation) and **O.Crypt** (requiring the encryption of persistently stored TSF and user data of the TOE). In addition the physical protection provided by the environment (**OE.PhysicalProtection**) and the SRV (**OE.TrustedAdmins**) who could realize a physical manipulation contribute to counter this threat.

The aspect of a remote attacker is covered by **O.Firewall** as this objective ensures that an adequate level of protection is realized against attacks from the WAN side.

4.3.2.10 T.Privacy

The threat **T.Privacy** is primarily addressed by the security objectives **O.Meter, O.Crypt** and **O.Firewall** as these objective ensures that the TOE will only distribute meter data to external market participants in the WAN as defined in the corresponding processing profiles and that the data will be protected for the transfer. **OE.Profile** is present to ensure that the processing profiles are obtained from a trustworthy and reliable source only.

O.Access defines that the TOE shall control the access of users to information via the external interfaces.

Finally, **O.ConcealWAN** ensures that an attacker cannot obtain the relevant information for this threat by observing external characteristics of the information flow.

4.3.3 Coverage of organizational security policies

The following sections provide more detailed information about how the security objectives for the environment and the TOE cover the organizational security policies.

4.3.3.1 OSP.SM

The organizational security policy **OSP.SM** that mandates that the TOE utilizes the services of a certified security module is directly addressed by the security objectives **OE.SM** and **O.Crypt**. The objective **OE.SM** addresses the functions that the security module shall be utilized for as defined in **OSP.SM** and also requires a certified security module. **O.Crypt** defines the cryptographic functionalities for the TOE itself. In this context it has to be ensured that the security module is operated in accordance with its guidance documentation.

4.3.3.2 OSP.Log

The organizational security policy **OSP.Log** that mandates that the TOE maintains an audit log is directly addressed by the security objective for the TOE **O.Log**.

O.Access contributes to the implementation of the OSP as it defines that also GWAs are not allowed to read/modify all data. This is of specific importance to ensure the confidentiality and integrity of the log data as is required by the **OSP.Log**.

4.3.3.3 OSP.KeyGenService

The organizational security policy **OSP.KeyGenService** that mandates that the TOE provides a key generation service is directly addressed by the security objective for the TOE **O.KeyGenService.**

O.Access contributes to the implementation of the OSP as it supports that the access of the generated key and certificates is limited to the respective external entities.

O.Crypt defines the required cryptographic functionality.

4.3.4 Coverage of assumptions

The following sections provide more detailed information about how the security objectives for the environment cover the assumptions.

4.3.4.1 A.ExternalPrivacy

The assumption **A.ExternalPrivacy** is directly and completely covered by the security objective **OE.ExternalPrivacy**. The assumption and the objective for the environment are drafted in a way that the correspondence is obvious.

4.3.4.2 A.TrustedAdmins

The assumption **A.TrustedAdmins** is directly and completely covered by the security objective **OE.TrustedAdmins**. The assumption and the objective for the environment are drafted in a way that the correspondence is obvious.

4.3.4.3 A.PhysicalProtection

The assumption **A.PhysicalProtection** is directly and completely covered by the security objective **OE.PhysicalProtection**. The assumption and the objective for the environment are drafted in a way that the correspondence is obvious.

4.3.4.4 A.Profile

The assumption **A.Profile** is directly and completely covered by the security objective **OE.Profile.** The assumption and the objective for the environment are drafted in a way that the correspondence is obvious.

4.3.4.5 A.Update

The assumption **A.Update** is directly and completely covered by the security objective **OE.Update.** The assumption and the objective for the environment are drafted in a way that the correspondence is obvious.

4.3.4.6 A.Network

The assumption **A.Network** is directly and completely covered by the security objective **OE.Network.** The assumption and the objective for the environment are drafted in a way that the correspondence is obvious.

4.3.4.7 A.Keygen

The assumption **A.Keygen** is directly and completely covered by the security objective **OE.Keygen.** The assumption and the objective for the environment are drafted in a way that the correspondence is obvious.

4.3.4.8 A.Delivery

The assumption **A.Delivery** is directly and completely covered by the security objective **OE.Delivery.** The assumption and the objective for the environment are drafted in a way that the correspondence is obvious.

4.3.4.9 A.IndustrialMeterHAN

The assumption **A.IndustrialMeterHAN** is directly and completely covered by the security objective **OE.IndustrialMeterHAN.** The assumption and the objective for the environment are drafted in a way that the correspondence is obvious.

5 Extended component definition

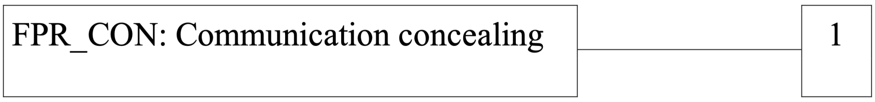
5.1 Communication concealing (FPR_CON)

The additional family communication concealing (FPR_CON) of the class FPR (Privacy) is defined here to describe the specific IT security functional requirements of the TOE. The TOE shall prevent attacks against personally identifiable information (PII) of the consumer that may be obtained by an attacker by observing the encrypted communication of the TOE with remote entities.

5.1.1 Family behaviour

This family defines requirements to mitigate attacks against communication channels in which an attacker tries to obtain privacy relevant information based on characteristics of an encrypted communication channel. Examples include but are not limited to an analysis of the frequency of communication or the transmitted workload.

5.1.2 Component levelling



5.1.3 Management

The definition of the interval in FPR_CON.1.2, if definable within the operational phase of the TOE, is the only action that could be considered for the management functions in FMT.

5.1.4 Audit

There are no auditable events foreseen.

5.1.5 Communication concealing (FPR_CON.1)

Hierarchical to: No other components.

Dependencies: No dependencies.

FPR_CON.1.1 **The TSF shall enforce the** [assignment: ***information flow policy***] **in order to ensure that no personally identifiable information (PII) can be obtained by an analysis of** [**assignment:** ***characteristics of the information flow that need to be concealed***].

FPR_CON.1.2 **The TSF shall connect to** [**assignment:** ***list of external entities***] **in intervals as follows** [**selection, choose one of:** ***weekly, daily, hourly, [assignment: other interval]***] **to conceal the data flow.**

6 Security requirements

6.1 Overview

This chapter describes the security functional requirements (SFRs) and the security assurance requirements (SARs) which have to be fulfilled by the TOE. Those requirements comprise functional components from [CC:2022] Part 2 and the assurance components as defined in [CC:2022] Part 3 for the evaluation assurance level 4 (EAL4) as defined in [CC:2022] Part 5.

The following notations are used:

- **Refinement** operation (denoted by **bold text**): is used to add details to a requirement, and thus further restricts a requirement. In case that a word has been deleted from the original text this refinement is indicated by ~~**crossed out bold text**~~.
- **Selection** operation (denoted by underlined text): is used to select one or more options provided by the [CC:2022] in stating a requirement.
- **Assignment** operation (denoted by *italicized text*): is used to assign a specific value to an unspecified parameter, such as the length of a password.
- **Iteration** operation: are identified with a suffix in the name of the SFR (e.g., FAU_GEN.1/SYS).

For selections left to the ST author, "quotation marks" around an option of the selection are used when a comma is contained in that option.

It should be noted that the requirements in the following sections are not necessarily be ordered alphabetically. Where useful, the SFRs have been grouped.

▸Table 6.1 lists all SFRs of this PP. Optional SFRs are denoted by "(optional)".

Class FAU: Security audit	
▸FAU_ARP.1/SYS	Security alarms for system log
▸FAU_GEN.1/SYS	Audit data generation for system log
▸FAU_SAA.1/SYS	Potential violation analysis for system log
▸FAU_SAR.1/SYS	Audit review for system log
▸FAU_STG.5/SYS	Prevention of audit data loss for system log
▸FAU_GEN.1/CON	Audit data generation for consumer log
▸FAU_SAR.1/CON	Audit review for consumer log
▸FAU_STG.5/CON	Prevention of audit data loss for consumer log
▸FAU_GEN.1/CAL	Audit data generation for calibration log
▸FAU_SAR.1/CAL	Audit review for calibration log
▸FAU_STG.5/CAL	Prevention of audit data loss for calibration log
▸FAU_GEN.2	User identity association
▸FAU_STG.3	Guarantees of audit data availability
Class FCS: Cryptographic support	
▸FCS_CKM.5/TLS	Cryptographic key derivation for TLS
▸FCS_COP.1/AES	Cryptographic operation with AES-CBC, AES-GCM and AES-CCM
▸FCS_COP.1/MTRCMAC	Cryptographic operation with AES-CMAC for secure communication with meters
▸FCS_COP.1/CMSCMAC	Cryptographic operation with AES-CMAC for CMS
▸FCS_COP.1/HMAC	Cryptographic operation with HMAC
▸FCS_CKM.5/CMAC	Cryptographic key derivation with AES-CMAC
▸FCS_COP.1/HASH	Cryptographic operation: hashing

▸FCS_COP.1/MEM	Cryptographic operation, encryption of TSF and user data
▸FCS_CKM.5/X963	Cryptographic key derivation with X9.63
▸FCS_COP.1/AESWRAP	Cryptographic operation with AES key wrap
▸FCS_CKM.1/SERVICE	Cryptographic key generation for key distribution to HAN and LMN
▸FCS_CKM.6	Timing and event of cryptographic key destruction
Class FDP: User data protection	
▸FDP_ACC.2	Complete access control
▸FDP_ACF.1	Security attribute-based access control
▸FDP_IFC.2	Complete information flow control
▸FDP_IFF.1	Simple security attributes
▸FDP_RIP.2	Full residual information protection
▸FDP_SDI.2	Stored data integrity monitoring and action
Class FIA: Identification and authentication	
▸FIA_AFL.1	Authentication failure handling
▸FIA_ATD.1	User attribute definition
▸FIA_UAU.1	Timing of authentication
▸FIA_UAU.5	Multiple authentication mechanisms
▸FIA_UID.1	Timing of identification
▸FIA_USB.1	User-subject binding
Class FMT: Security management	
▸FMT_MOF.1	Management of security functions behaviour
▸FMT_MTD.1	Management of TSF data
▸FMT_SMF.1	Specification of management functions
▸FMT_SMR.1	Security roles
Class FPR: Privacy	
▸FPR_CON.1	Communication concealing
▸FPR_PSE.1	Pseudonymity
Class FPT: Protection of the TSF	
▸FPT_FLS.1	Failure with preservation of secure state
▸FPT_PHP.1	Passive detection of physical attack
▸FPT_RPL.1	Replay detection
▸FPT_STM.1	Reliable time stamps
▸FPT_STM.2	Time source
▸FPT_TST.1	TSF self-testing
Class FTP: Trusted path/channels	
▸FTP_PRO.1/TLS12	Trusted channel protocol for TLSv1.2
▸FTP_PRO.2/TLS12	Trusted channel establishment for TLSv1.2
▸FTP_PRO.3/TLS12	Trusted channel data protection for TLSv1.2
▸FTP_PRO.1/TLS13	Trusted channel protocol for TLSv1.3 (optional)
▸FTP_PRO.2/TLS13	Trusted channel establishment for TLSv1.3 (optional)
▸FTP_PRO.3/TLS13	Trusted channel data protection for TLSv1.3 (optional)

▸FTP_PRO.1/SYM	Trusted channel protocol for unidirectional communication with meters in LMN
▸FTP_PRO.2/SYM	Trusted channel establishment for unidirectional communication with meters in LMN
▸FTP_PRO.3/SYM	Trusted channel data protection for unidirectional communication with meters in LMN
▸FTP_PRO.1/CMS	Trusted channel protocol for content data encryption
▸FTP_PRO.2/CMS	Trusted channel establishment for content data encryption
▸FTP_PRO.3/CMS	Trusted channel data protection for content data encryption

Table 6.1 List of security functional requirements

6.2 Class FAU: Security audit

6.2.1 Overview

A TOE compliant to this PP shall implement three types of logs: the system log, the consumer log and the calibration log. ▸Table 6.2 provides an overview over the three audit logs before the following sections introduce the SFRs modeling the functionality required for these audit logs. Note that for each consumer, a separate instantiation of a consumer log exists.

	System log	Consumer log	Calibration log
Purpose	• Log and inform the GWA/SRV about all security relevant events • Log all events as defined by CC for the used SFR • Log all system relevant events on specific functionality • Automated alarms in case of a cumulation of certain events • Log information about the status of the TOE	• Inform the consumer about the attributes associated with their user identity • Inform the consumer about the TOE version, identity as well as meter identities and external entities associated with the consumer's user identity • Inform the consumer about information flow events associated with the meter data associated with the consumer's user identity • Inform the consumer about status events and errors associated with the consumer's user identity	• Log changes that are relevant for the calibration of the TOE
Data	• As defined by [CC:2022] Part 2 • Augmented by specific events for the security functions	• The consumer's user identity • The TOE version (including hardware and software version) and identity • Identities of meters and of external entities in the WAN that are allowed to receive meter data associated with the consumer's user identity • Information about information flows of meter data associated with the consumer's user identity to external entities in the WAN • Information about status events and errors relevant for the consumer • Information about management and configuration of attributes, data, processing profiles and communication profiles associated with the consumer's user identity	• Calibration relevant data only • Information on successful firmware updates

	System log	Consumer log	Calibration log
Access	• Access by authorized GWA and via WAN only • Events may only be deleted by an authorized GWA via WAN • Read access by authorized SRV via HAN-CON or HAN-CLS only	• Read access by authorized consumer and via HAN-CON or HAN-CLS only to the data associated with that consumer	• Read access by authorized GWA via WAN or by authorized SRV via HAN-CON or HAN-CLS only. • Deletion of events by an authorized GWA via WAN or by an authorized SRV via HAN-CON or HAN-CLS only. The deleted data have to be exported beforehand.
Deletion	• Ring buffer. • The availability of data has to be ensured for a sufficient amount of time • Overwriting old events is possible if the memory is full	• Ring buffer. • The availability of data has to be ensured for a sufficient amount of time • Overwriting old events is possible if the memory is full provided that these events are older thant 15 months.	• If the calibration log is full, the TOE has to reversibly stop operation. • It has to be ensured that the calibration log data are available for three years counting from the end of the year of generation of said events. This availability does not need to be provided by the TOE; it may be provided by the GWA and their backend systems. • Active deletion of events by the GWA or SRV is possible before the end of the above period if they exported the data beforehand. The TOE has to ensure that events logging successful firmware updates are not deleted.

Table 6.2 Overview over audit processes

6.2.2 Security Requirements for the system log

6.2.2.1 FAU_ARP.1/SYS: Security alarms for system log

FAU_ARP.1.1/SYS The TSF shall ~~take~~ [*inform an authorized GWA and [assignment: list of actions]*] upon detection of a potential security violation.

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 fulfilled by ▸FAU_SAA.1/SYS

6.2.2.2 FAU_GEN.1/SYS: Audit data generation for system log

FAU_GEN.1.1/SYS The TSF shall be able to generate audit data of the following auditable events:

a. Start-up and shutdown of the audit functions;

b. All auditable events for the [not specified] level of audit;

c. [*All events listed in ▸Table 6.3, and [assignment: other non-privacy relevant auditable events]*]

FAU_GEN.1.2/SYS The TSF shall record within the audit data at least the following information:

a. Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome[19] (success or failure) of the event;

b. For each auditable event type, based on the auditable event definitions of the functional components included in the PP~~**, PP-Module, functional package or ST,**~~ [*additional information as listed in* ▸*Table 6.3 and [assignment: additional events or none]*].

Hierarchical to: No other components.

Dependencies: FPT_STM.1 ▸directly fulfilled

Based on SFR	*Event*	*Additional information*
▸FAU_ARP.1/SYS	Actions taken due to potential security violations.	-
▸FAU_SAA.1/SYS	Enabling and disabling of any analysis mechanisms	-
▸FAU_STG.5/SYS	Actions and warnings taken due to the audit storage failure	At least “Critical log capacity before overwriting 1st event” and “1st event overwritten” or similar.
▸FAU_STG.5/CON	Actions and warnings taken due to the audit storage failure	At least “Critical log capacity before overwriting 1st event” and “1st event overwritten” or similar.
▸FAU_SAR.1/CAL	Reading of information from the audit records.	Concerning the calibration log, every (read) access should be logged.
▸FAU_STG.5/CAL	Actions and warnings taken due to the audit storage failure	At least “Critical log capacity before overwriting 1st event” and “Capacity exhausted, initiating secure state” or similar.
▸FCS_COP.1/AES	Failure, and the chosen cryptographic primitives.	-
▸FCS_COP.1/MTRCMAC	Failure, and the chosen cryptographic primitives.	-
▸FCS_COP.1/HMAC	Failure, and the chosen cryptographic primitives.	-
▸FCS_COP.1/HASH	Failure, and the chosen cryptographic primitives.	-
▸FCS_COP.1/MEM	Failure, and the chosen cryptographic primitives.	-
▸FCS_COP.1/AESWRAP	Failure, and the chosen cryptographic primitives.	-
▸FCS_CKM.5/TLS	Failure, and the chosen cryptographic primitives.	-
▸FCS_CKM.5/CMAC	Failure of the specific activity. The object attribute(s), and object value(s) excluding any sensitive information (e.g., secret or private keys).	-
▸FCS_CKM.5/X963	Failure of the specific activity. The object attribute(s), and object value(s) excluding any sensitive information (e.g., secret or private keys).	-

[19] There might be auditable events that do not have an outcome. In this case, the outcome is not required.

Based on SFR	*Event*	*Additional information*
▸FCS_CKM.1/SERVICE	Failure of the specific activity. The object attribute(s), and object value(s) excluding any sensitive information (e.g., secret or private keys).	-
▸FCS_CKM.6	Failure of the specific activity. The object attribute(s), and object value(s) excluding any sensitive information (e.g., secret or private keys).	-
▸FDP_ACF.1	All requests to perform an operation on an object covered by the SFP.	-
▸FDP_IFF.1	All errors and warnings resulting on requests for information flow.	-
▸FDP_SDI.2	Failed attempts to check the integrity of user data.	-
▸FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent, if appropriate, restoration to the normal state.	-
▸FIA_UAU.1 ▸FIA_UAU.5 ▸FIA_UID.1	Every authentication or identification attempt with result and corresponding user id where applicable.	-
▸FIA_USB.1	Success and failure of binding of user security attributes to a subject (e.g., success or failure to create a subject).	-
▸FMT_MOF.1 ▸FMT_SMF.1	Use of the management functions and corresponding user id. All modifications in the behaviour of the functions in the TSF. Error messages in case of unallowed/undefined modification attempts.	Only functions defined in FMT_SMF.1 should be executable. All further attempts should lead to an error message.
▸FMT_MTD.1	All modifications to the values of TSF data.	-
▸FPT_FLS.1	Failure of the TSF.	-
▸FPT_STM.1	Changes to the time.	-
▸FPT_STM.2	Changes to the time source.	-
▸FPT_TST.1	Trigger, execution and result of a self-test.	-
▸FTP_PRO.1/TLS12	All attempted uses of the trusted channel, identification of the initiator and target of all trusted channel attempts.	Not all functions transferred via the trusted channel must be logged.
▸FTP_PRO.2/TLS12	All authentication attempts.	-
▸FTP_PRO.3/TLS12	Failures when attempting to verify channel properties in FTP_PRO.3.2/TLS12.	Failures due to replayed TLS messages do not need to be logged.
▸FTP_PRO.1/TLS13	All attempted uses of the trusted channel, identification of the initiator and target of all trusted channel attempts.	Not all functions transferred via the trusted channel must be logged.
▸FTP_PRO.2/TLS13	All authentication attempts.	-
▸FTP_PRO.3/TLS13	Failures when attempting to verify channel properties in FTP_PRO.3.2/TLS13.	Failures due to replayed TLS messages do not need to be logged.
▸FTP_PRO.1/SYM	All attempted uses of the trusted channel, identification of the initiator and target of all trusted channel attempts.	Not all functions transferred via the trusted channel must be logged.

Based on SFR	*Event*	*Additional information*
▸FTP_PRO.2/SYM	All authentication attempts.	-
▸FTP_PRO.3/SYM	Failures when attempting to verify channel properties in FTP_PRO.3.2/SYM.	-
▸FTP_PRO.1/CMS	Failures when attempting to decrypt a CMS container.	-
▸FTP_PRO.3/CMS	Failures when attempting to validate the signature of a CMS container.	-

Table 6.3 Events for system log

6.2.2.3 FAU_SAA.1/SYS: Potential violation analysis for system log

FAU_SAA.1.1/SYS The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2/SYS The TSF shall enforce the following rules for monitoring audited events:

a. Accumulation or combination of [assignment: *subset of defined auditable events*] known to indicate a potential security violation;

b. [assignment: *any other rules*].

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 fulfilled by ▸FAU_GEN.1/SYS

Application Note 13 The specific events that shall be analyzed in the system log in order to ensure a correct operation of the TOE highly depend on the specific implementation and application of the TOE; as such the authors of the ST will have to complete the operations in ▸FAU_SAA.1/SYS. At least all types of failures in the TSF as listed in ▸FPT_FLS.1 should be recognized as potential violation by the TOE.

6.2.2.4 FAU_SAR.1/SYS: Audit review for system log

FAU_SAR.1.1/SYS The TSF shall provide [*only authorized GWAs via the WAN interface and authorized SRVs via the HAN-CON and HAN-CLS interface*] with the capability to read [*any information*] from the **system** audit data.

FAU_SAR.1.2/SYS The TSF shall provide the audit data in a manner suitable for the user to interpret the information.

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 fulfilled by ▸FAU_GEN.1/SYS

6.2.2.5 FAU_STG.5/SYS: Prevention of audit data loss for system log

FAU_STG.5.1/SYS The TSF shall [overwrite the oldest stored audit records], [assignment: *other actions to be taken in case of audit storage failure and conditions for the actions*] if the **system** audit data storage is full.

Hierarchical to: FAU_STG.4 Action in case of possible audit data loss

Dependencies: FAU_STG.2 fulfilled by ▸FAU_STG.3

FAU_GEN.1 fulfilled by ▸FAU_GEN.1/SYS

Application Note 14 The size of the audit trail that is available before the oldest events get overwritten is configurable for the GWA.

6.2.3 Security requirements for the consumer log

6.2.3.1 FAU_GEN.1/CON: Audit data generation for consumer log

FAU_GEN.1.1/CON The TSF shall be able to generate audit data of the following auditable events:

a. Start-up and shutdown of the audit functions;

b. All auditable events for the [not specified] level of audit;

c. [*all audit events as listed in ▸Table 6.4 and [assignment: additional events or none]*]

FAU_GEN.1.2/CON The TSF shall record within the audit data at least the following information:

a. Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome[20] (success or failure) of the event;

b. For each auditable event type, based on the auditable event definitions of the functional components included in the PP~~, **PP-Module, functional package or ST,**~~ [*additional information as listed in ▸Table 6.4 and [assignment: additional events or none]*].

Hierarchical to: No other components.

Dependencies: FPT_STM.1 ▸directly fulfilled

Application Note 15 The possibility for the ST author to specify additional events in ▸FAU_GEN.1.1/CON has been specifically introduced to allow that a more detailed set of information about the consumption or production of a certain commodity is audited (e.g. to allow a consumer to control the consumption or production on a granular level). Such information shall primarily be captured in the consumer log as this log has the appropriate permissions associated to ensure that only the consumer can review the events.

Further, the ST author shall consider the descriptions in ▸Section 1.4.6.7 to decide whether additional information needs to be audited for a specific TOE.

Event	*Additional information*
Any change to a processing profile	• In case of a new processing profile, the whole processing profile • In case of a change of an existing processing profile, the ID of the profile and the updated values of the processing profile • In case of a deleted processing profile, the ID of the profile
Submission of meter data to an external market participant for data access	• The number of meter data and interval of the meter data that were sent as well as the receiving external market participant ID • For on-demand deliveries, i.e., where the submission is not specified as periodical in the corresponding processing profile (e.g. triggering by the GWA, or reaching a threshold), the date of the delivery and the external market participant ID • The requirement to log the periodical submission of meter data depends on the processing profile. For on-demand deliveries, the logging is always necessary.
Any administrative action performed relevant to the specific user	-

[20] There might be auditable events that do not have an outcome. In this case, the outcome is not required.

Event	*Additional information*
Relevant system status information including relevant errors This includes at least all events defined in ▸Table 6.3 for the following SFRs: • FAU_STG.5/CON, • FAU_STG.5/CAL, • FDP_SDI.2, • FIA_AFL.1, • FMT_MTD.1, • FPT_FLS.1, • FPT_STM.1, and • FPT_STM.2, and • FPT_TST.1.	• In terms of FIA_AFL.1 only visible for the perpetrator of the failure, where applicable, and with a general entry in all other cases.

Table 6.4 Events for consumer log

6.2.3.2 FAU_SAR.1/CON: Audit review for consumer log

FAU_SAR.1.1/CON The TSF shall provide [*only authorized consumers via the HAN-CLS or HAN-CON interface*] with the capability to read [*all information that are related to them*] from the **consumer** audit data.

FAU_SAR.1.2/CON The TSF shall provide the audit data in a manner suitable for the user to interpret the information.

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 fulfilled by ▸FAU_GEN.1/CON

Application Note 16 ▸FAU_SAR.1.2/CON shall ensure that the consumer is able to interpret the information that is provided to him in a way that allows him to verify the invoice.

6.2.3.3 FAU_STG.5/CON: Prevention of audit data loss for consumer log

FAU_STG.5.1/CON The TSF shall [overwrite the oldest stored audit records], [assignment: *other actions to be taken in case of audit storage failure and conditions for the actions*] if the **consumer** audit data storage is full **and these audit records are older than 15 months**.

Hierarchical to: FAU_STG.4 Action in case of possible audit data loss

Dependencies: FAU_STG.2 fulfilled by ▸FAU_STG.3

FAU_GEN.1 fulfilled by ▸FAU_GEN.1/CON

Application Note 17 The size of the audit trail that is available before the oldest events get overwritten is configurable for the GWA as long as the national requirements in the context of the TOE consumer log are fulfilled.

6.2.4 Security Requirements for the calibration log

6.2.4.1 FAU_GEN.1/CAL: Audit data generation for calibration log

FAU_GEN.1.1/CAL The TSF shall be able to generate audit data of the following auditable events:

a. Start-up and shutdown of the audit functions;

b. All auditable events for the [not specified] level of audit;

c. [assignment: *all audit events as listed in ▸Table 6.5 and [assignment: all calibration-relevant information]*]

FAU_GEN.1.2/CAL The TSF shall record within the audit data at least the following information:

a. Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome[21] (success or failure) of the event;

b. For each auditable event type, based on the auditable event definitions of the functional components included in the PP~~, PP-Module, functional package or ST,~~ [*all calibration-relevant information, additional information as listed in* ▸*Table 6.5, and [assignment: other audit relevant information]*].

Hierarchical to: No other components.

Dependencies: FPT_STM.1 ▸directly fulfilled

Application Note 18 The calibration log serves to fulfill national requirements in the context of the calibration of the TOE. The ST author shall consider the regulations from the national calibration authority in [BSI-TR-03109-1] in order to decide about the amount of information that needs to be available for the calibration log.

Event	*Additional information*
All events defined in ▸Table 6.3 for the following SFRs: • FAU_STG.5/CAL, • FDP_SDI.2, • FPT_FLS.1, • FPT_STM.1, and • FPT_STM.2, and • FPT_TST.1.	For FAU_STG.5/CAL, this includes all actions taken due to the audit storage failure in the calibration log (after calibration log is available again).
All events concerning a firmware update	This includes but is not limited to successful and unsuccessful firmware updates.

Table 6.5 Events for calibration log

6.2.4.2 FAU_SAR.1/CAL: Audit review for calibration log

FAU_SAR.1.1/CAL The TSF shall provide [*only authorized GWAs via WAN and authorized SRVs via HAN-CLS or HAN-CON*] with the capability to read [*any information*] from the **calibration** audit data.

FAU_SAR.1.2/CAL The TSF shall provide the audit data in a manner suitable for the user to interpret the information.

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 fulfilled by ▸FAU_GEN.1/CAL

6.2.4.3 FAU_STG.5/CAL: Prevention of audit data loss for calibration log

FAU_STG.5.1/CAL The TSF shall [ignore audited events], [*reversibly stop the operation of the TOE and inform the GWA*] if the **calibration** audit data storage is full.

Hierarchical to: FAU_STG.4 Action in case of possible audit data loss

Dependencies: FAU_STG.2 fulfilled by ▸FAU_STG.3

FAU_GEN.1 fulfilled by ▸FAU_GEN.1/CAL

Application Note 19 As outlined in the introduction, it has to be ensured that the events of the calibration log are available for three years counting from the end of the year of generation of said events according to national regulations. The availability of these data may be provided by the GWA instead of the TOE if they export the data and store them outside the TOE. A deletion of certain events in the calibration log by the GWA and

[21] There might be auditable events that do not have an outcome. In this case, the outcome is not required.

the SRV is therefore permitted, however, they have to ensure that that they exported the audit trail beforehand, see ▸FMT_MTD.1.

Nevertheless, the developer shall consider choosing a sufficient size so that the availability of all required events in the calibration log is given.

6.2.5 Security requirements for all logs

6.2.5.1 Security audit data generation (FAU_GEN)

6.2.5.1.1 FAU_GEN.2: User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 fulfilled by ▸FAU_GEN.1/SYS, ▸FAU_GEN.1/CON and ▸FAU_GEN.1/CAL

FIA_UID.1 ▸directly fulfilled

Application Note 20 Please note that ▸FAU_GEN.2 applies to all audit logs, the system log, the calibration log, and the consumer log.

6.2.5.2 Security audit event storage (FAU_STG)

6.2.5.2.1 FAU_STG.3: Guarantees of audit data availability

FAU_STG.3.1 The TSF shall protect the stored audit data in ~~**the**~~ **all** audit trail**s** from unauthorized deletion.

FAU_STG.3.2 The TSF shall be able to [prevent] unauthorized modifications to the stored audit data in ~~**the**~~ **all** audit trail**s**.

FAU_STG.3.3 The TSF shall ensure that [assignment: *metric for saving audit records*] stored audit data will be maintained when the following conditions occur: [audit data storage exhaustion, failure].

Hierarchical to: FAU_STG.2 Protected audit data storage

Dependencies: FAU_GEN.1 fulfilled by ▸FAU_GEN.1/SYS, ▸FAU_GEN.1/CON and ▸FAU_GEN.1/CAL

Application Note 21 The ST author shall consider the regulations from the national calibration authority [BSI-TR-03109-1] in order to decide about the amount of information that needs to be available for the requirement in ▸FAU_STG.3.3 for each audit log. Additionally, it has to be ensured that log entries are available to the corresponding user role as long as required to fulfil the needs of the user role and retention period potentially given by the legislator.

6.3 Class FCS: Cryptographic support

6.3.1 Overview

The TOE together with the security module provide cryptographic support as depicted in ▸Table 1.3. The cryptographic primitives provided by the TOE are modeled via SFRs in this section. The cryptographic primitives provided by the security module are ECDSA for signature generation and verification, ECKA-DH and ECKA-EG for key agreement as well as the generation of random numbers. The security module further provides secure storage for keys.

To link the cryptographic primitives of the TOE to the protocols used for secure communication with external entities, FTP_PRO is used:

- Details concerning the TLS protocol v1.2 are modelled in ▸FTP_PRO.1/TLS12, ▸FTP_PRO.2/TLS12 and ▸FTP_PRO.3/TLS12.
- Details concerning the protocol used for the unidirectional communication with meters based on symmetric encryption are modelled in ▸FTP_PRO.1/SYM, ▸FTP_PRO.2/SYM and ▸FTP_PRO.3/SYM. Note that the initial pre-shared key between meter and TOE has to be brought into the TOE before a communication is possible, see OE.Keygen.[22]
- Details concerning CMS as defined in [BSI-TR-03109-3] are modelled in ▸FTP_PRO.1/CMS, ▸FTP_PRO.2/CMS and ▸FTP_PRO.3/CMS.

These SFRs provide information on the precise usage of the cryptographic primitives for the respective protocols.

Application Note 22 If TLS v1.3 is implemented in the TOE, the ST author shall model it using the optional SFRs in ▸Section 6.9.4. If these optional SFRs are used, the operations of the SFRs in this section have to be fulfilled accordingly.

For the verification of wake-up messages, the TOE provides hashing as modelled in ▸FCS_COP.1/HASH.

For the encryption and decryption of persistent storage memory, see ▸FCS_COP.1/MEM.

The TOE provides a key generation service for devices in the HAN and LMN. For the generation of private-public key pairs and corresponding self-signed certificates, this key generation is modelled in ▸FCS_CKM.1/SERVICE. The derivation of a pre-shared key shared between TOE and meter is modelled in ▸FCS_CKM.5/CMAC.

6.3.2 FCS_CKM.1/SERVICE: Cryptographic key generation for key distribution to HAN and LMN

FCS_CKM.1.1/SERVICE The TSF shall generate cryptographic keys **for key distribution to HAN and LMN** in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm* ***for key distribution to HAN and LMN***] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [*[BSI-TR-03111]*].

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 unfulfilled, see ▸Table 6.13: SFR Dependencies. or

FCS_CKM.5 or

FCS_COP.1]

[FCS_RBG.1 or

FCS_RNG.1 unfulfilled, see ▸Table 6.13: SFR Dependencies.]

FCS_CKM.6 ▸directly fulfilled

Application Note 23 The TOE *shall only* use cryptographic specifications and algorithms as described in [BSI-TR-03109-3] and [BSI-TR-03111].

Application Note 24 When the RNG functionality is provided by the TOE itself, it shall be appropriately modelled by the ST author using the SFR FCS_RNG according to [CC:2022] Part 2 and considering [BSI-TR-03109-3]. In this case, the dependency on FCS_RNG.1 is fulfilled.

[22] Meters in the LMN may communicate unidirectionally or bidirectionally. For the details on the different communication scenarios and when they shall be used, see also [BSI-TR-03109-1] and [BSI-TR-03109-3]. As the TOE shall be interoperable with all kinds of meters, it requires the implementation of two means of communication: TLS-encrypted communication and communication based on symmetric encryption using AES.

6.3.3 FCS_CKM.5/TLS: Cryptographic key derivation for TLS

FCS_CKM.5.1/TLS The TSF shall derive cryptographic keys [*write MAC and write encryption keys for TLS v1.2, [selection, choose one of: traffic keys for TLS v1.3, none]*] from [*master secret, client random, server random*] in accordance with a specified key derivation algorithm [*the PRF defined by the cipher suites used for TLS v1.2 in ▸FTP_PRO.1.6/TLS12 with [selection: SHA-256, SHA-384] and [selection, choose one of: the HKDF defined by the cipher suites used for TLS v1.3 in ▸FTP_PRO.1.6/TLS13 with [selection: SHA-256, SHA-384], none]*] and specified cryptographic key sizes [*[selection: 128 bit for AES-128 and 256 bit for SHA256, 256 bit for AES-256 and 384 bit for SHA384]*] that meet the following: [*[RFC5246], [NIST-FIPS-197], [selection, choose one of: "RFC8446, RFC5869", none]*].

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 or

FCS_COP.1 fulfilled by ▸FCS_COP.1/AES]

FCS_CKM.6 ▸directly fulfilled

Application Note 25 The ST author shall complete the selection operations in accordance with [BSI-TR-03109-3], taking into account [BSI-TR-03109-1]. In particular, mandatory requirements according to [BSI-TR-03109-3] shall be selected. This also holds in the case that TLS v1.3 is implemented in the TOE.

6.3.4 FCS_CKM.5/CMAC: Cryptographic key derivation with AES-CMAC

FCS_CKM.5.1/CMAC The TSF shall derive cryptographic keys [

- *MAC and encryption keys for ▸FTP_PRO.2.3/SYM,*
- *shared secret between TOE and meter for ▸FTP_PRO.2.1/SYM*

] from [

- *master key, counter and meter ID for MAC and encryption keys*
- *master key, random number for shared secret*

] in accordance with a specified key derivation algorithm [*AES-CMAC according to ▸FCS_COP.1/MTRCMAC*] and specified cryptographic key sizes [*128 bit*] that meet the following: [*[RFC4493], [BSI-TR-03109-3]*].

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 or

FCS_COP.1 fulfilled by ▸FCS_COP.1/AES and ▸FCS_COP.1/MTRCMAC]

FCS_CKM.6 ▸directly fulfilled

Application Note 26 For details on the symmetric encryption and its usage, see [BSI-TR-03109-1] and [BSI-TR-03109-3].

6.3.5 FCS_CKM.5/X963: Cryptographic key derivation with X9.63

FCS_CKM.5.1/X963 The TSF shall derive cryptographic keys [*key encryption key for CMS*] from [*shared secret generated by the security module*] in accordance with a specified key derivation algorithm [*X9.63 with [selection: SHA-256, SHA-384, SHA-512]*] and specified cryptographic key sizes [*[selection: 128 bit, 192 bit, 256 bit]*] that meet the following: [*[BSI-TR-03111]*].

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 or

FCS_COP.1 fulfilled by ▸FCS_COP.1/AESWRAP]

FCS_CKM.6 ▸directly fulfilled

Application Note 27 The ST author shall complete the selection operations in accordance with [BSI-TR-03109-3], taking into account [BSI-TR-03109-1]. In particular, mandatory requirements according to [BSI-TR-03109-3] shall be selected.

6.3.6 FCS_COP.1/AES: Cryptographic operation with AES-CBC, AES-GCM and AES-CCM

FCS_COP.1.1/AES The TSF shall perform [*symmetric encryption and decryption*] in accordance with a specified cryptographic algorithm [*[selection: AES-CBC-128, AES-CBC-256, AES-GCM-128, AES-GCM-256, AES-CCM-128, [assignment: further cryptographic algorithms]]*] and cryptographic key sizes [*[selection: 128 bit, 256 bit, [assignment: further key sizes]]*] that meet the following: [*[NIST-FIPS-197], [NIST-SP800-38A], [NIST-SP800-38D], [selection, choose one of: [NIST-SP800-38C] , none]*].

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 or

FDP_ITC.2 or

FCS_CKM.1 or

FCS_CKM.5 fulfilled by ▸FCS_CKM.5/TLS]

FCS_CKM.6 ▸directly fulfilled

Application Note 28 The ST author shall complete the selection operations in accordance with [BSI-TR-03109-3], taking into account [BSI-TR-03109-1]. In particular, mandatory requirements according to [BSI-TR-03109-3] shall be selected. This also holds in the case that TLS v1.3 is implemented in the TOE.

6.3.7 FCS_COP.1/HMAC: Cryptographic operation with HMAC

FCS_COP.1.1/HMAC The TSF shall perform [*HMAC generation and verification*] in accordance with a specified cryptographic algorithm [*[selection: HMAC-SHA256, HMAC-SHA384]*] and cryptographic key sizes [*[selection: 256 bit, 384 bit]*] that meet the following: [*[RFC2104]*].

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 or

FDP_ITC.2 or

FCS_CKM.1 or

FCS_CKM.5 fulfilled by ▸FCS_CKM.5/TLS]

FCS_CKM.6 ▸directly fulfilled

Application Note 29 The ST author shall complete the selection operations in accordance with [BSI-TR-03109-3], taking into account [BSI-TR-03109-1]. In particular, mandatory requirements according to [BSI-TR-03109-3] shall be selected. This also holds in the case that TLS v1.3 is implemented in the TOE.

6.3.8 FCS_COP.1/MTRCMAC: Cryptographic operation with AES-CMAC for secure communication with meters

FCS_COP.1.1/MTRCMAC The TSF shall perform [*MAC generation and verification for secure communication with meters*] in accordance with a specified cryptographic algorithm [*AES-CMAC*] and cryptographic key sizes [*128 bit with [selection: 64 bit truncated MAC, 96 bit truncated MAC, 128 bit untruncated MAC]*] that meet the following: [*[RFC4493]*].

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 or

FDP_ITC.2 or

FCS_CKM.1 or

FCS_CKM.5 fulfilled by ▸FCS_CKM.5/CMAC]

FCS_CKM.6 ▸directly fulfilled

Application Note 30 The ST author shall complete the selection operations in accordance with [BSI-TR-03109-3], taking into account [BSI-TR-03109-1]. In particular, mandatory requirements according to [BSI-TR-03109-3] shall be selected.

6.3.9 FCS_COP.1/CMSCMAC: Cryptographic operation with AES-CMAC for CMS

FCS_COP.1.1/ CMSCMAC The TSF shall perform [*MAC generation and verification for CMS*] in accordance with a specified cryptographic algorithm [*AES-CMAC*] and cryptographic key sizes [*128 bit*] that meet the following: [*[RFC4493]*].

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 or

FDP_ITC.2 or

FCS_CKM.1 or

FCS_CKM.5 unfulfilled, see ▸Table 6.13: SFR Dependencies.]

FCS_CKM.6 ▸directly fulfilled

Application Note 31 The ST author shall complete the selection operations in accordance with [BSI-TR-03109-3], taking into account [BSI-TR-03109-1]. In particular, mandatory requirements according to [BSI-TR-03109-3] shall be selected.

Application Note 32 The encryption and MAC keys used for content data encryption for CMS according to [BSI-TR-03109-3] are randomly generated and on-time for the purpose of content data encryption. The method of key generation is left to the ST author. The ST author shall, depending on the implementation of the TOE, use an existing SFR or add a new (iteration of an) SFR. In case the dependency is not fulfilled by the TOE itself, a rationale for the missing dependency needs to be added to the corresponding section (see ▸Section 6.11), and an appropriate process of key generation in the environment and import to the TOE needs to be described and evaluated according to ALC_LCD.1. See also the information in ▸Section 6.3.1

6.3.10 FCS_COP.1/AESWRAP: Cryptographic operation with AES key wrap

FCS_COP.1.1/ AESWRAP The TSF shall perform [*key wrapping for CMS*] in accordance with a specified cryptographic algorithm [*AES key wrap*] and cryptographic key sizes [*[selection: 128 bit, 192 bit, 256 bit]*] that meet the following: [*[RFC3565], [RFC3394], [BSI-TR-03111]*].

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 or

FDP_ITC.2 or

FCS_CKM.1 or

FCS_CKM.5 fulfilled by ▸FCS_CKM.5/X963]

FCS_CKM.6 ▸directly fulfilled

Application Note 33 The ST author shall complete the selection operations in accordance with [BSI-TR-03109-3], taking into account [BSI-TR-03109-1]. In particular, mandatory requirements according to [BSI-TR-03109-3] shall be selected.

6.3.11 FCS_COP.1/HASH: Cryptographic operation: hashing

FCS_COP.1.1/HASH The TSF shall perform [*hashing for signature creation and verification*] in accordance with a specified cryptographic algorithm [*[selection: SHA-256, SHA-384, SHA-512]*] and cryptographic key sizes [*none*] that meet the following: [*[NIST-FIPS-180-4]*].

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 or

FDP_ITC.2 or

FCS_CKM.1 unfulfilled, see ▸Table 6.13: SFR Dependencies. or

FCS_CKM.5]

FCS_CKM.6 ▸directly fulfilled

Application Note 34 The TOE is only responsible for hashing of data in the context of digital signatures. The actual signature operation and the handling (i.e. protection) of the cryptographic keys in this context is performed by the security module.

Application Note 35 The TOE *shall only* use cryptographic specifications and algorithms as described in [BSI-TR-03109-3].

6.3.12 FCS_COP.1/MEM: Cryptographic operation, encryption of TSF and user data

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

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 or

FDP_ITC.2 or

FCS_CKM.1 unfulfilled, see ▸Table 6.13: SFR Dependencies. or

FCS_CKM.5]

FCS_CKM.6 ▸directly fulfilled

Application Note 36 The key generation for this SFR is left to the ST author, hence, the dependency for FCS_CKM.1 remains unfulfilled in this PP. The ST author shall, depending on the implementation of the TOE, use an existing SFR or add a new (iteration of an) SFR. In case the dependency is not fulfilled by the TOE itself, a rationale for the missing dependency needs to be added to the corresponding section (see ▸Section 6.11), and an appropriate process of key generation in the environment and import to the TOE needs to be described and evaluated according to ALC_LCD.1.

Application Note 37 The TOE shall encrypt its local TSF data and user data while it is not in use (i.e. while stored in a persistent memory). The exact approach to handle the key that is used for this functionality is left to the ST author. However, the ST author is motivated to consider the use of the build-in security module to store the symmetric key that is used for the encryption of TSF and user data.

Application Note 38 [BSI-TR-02102-1] should be considered when a cryptographic algorithm is chosen.

6.3.13 FCS_CKM.6: Timing and event of cryptographic key destruction

FCS_CKM.6.1 The TSF shall destroy [assignment: *list of cryptographic keys (including keying material)*] when [selection: *no longer needed, [assignment: other circumstances for key or keying material destruction]*].

FCS_CKM.6.2 The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method [assignment: *cryptographic key destruction method*] that meets the following: [assignment: *list of standards*].

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 or

FDP_ITC.2 or

FCS_CKM.1 fulfilled by ▸FCS_CKM.1/SERVICE or

FCS_CKM.5 fulfilled by ▸FCS_CKM.5/TLS, ▸FCS_CKM.5/CMAC and ▸FCS_CKM.5/X963]

Application Note 39 The ST author shall in particular include all ephemeral and session keys that are no longer in use as well as the private keys generated for the key generation service in ▸FCS_CKM.1/SERVICE after they have been transferred to the devices in the HAN or LMN.

Application Note 40 Please note that in contrast to the requirement ▸FDP_RIP.2, the mechanisms implementing the requirement from ▸FCS_CKM.6 shall be suitable to avoid attackers with physical access to the TOE from accessing the keys after they are no longer used.

6.4 Class FDP: User data protection

6.4.1 Overview

The security functional requirements in this section define a set of security functional policies (SFPs) as well as model the handling of residual information present on the TOE as well as the monitoring of stored user data.

Security functional policies

The SMGW access SFP is an access control policy to control the access to objects under the control of the TOE. The details of this access control policy highly depend on the concrete application of the TOE. The access control policy is described in more detail in [BSI-TR-03109-1].

The SMGW information flow SFP implements an information flow policy to fulfill the objective O.Firewall and O.Meter. All requirements concerning the information flow between the TOE and the different networks, as well as the handling of meter data in particular, are defined in this policy.

6.4.2 SMGW access SFP

6.4.2.1 FDP_ACC.2: Complete access control

FDP_ACC.2.1 The TSF shall enforce the [*SMGW access SFP*] on [

subjects: authorized GWA, SRV, CON, CLS, meter

objects: all assets as defined in ▸Table 3.2 and all TSF data

] 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.

Hierarchical to: FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 ▸directly fulfilled

6.4.2.2 FDP_ACF.1: Security attribute-based access control

FDP_ACF.1.1 The TSF shall enforce the [*SMGW access SFP*] to objects based on the following: [

subjects: authorized GWA, authorized SRV, authorized CON, authorized CLS, authorized meter, unauthorized external entity, [assignment: additional subjects or none] *objects: all assets as defined in ▸Table 3.2 and all TSF data, [assignment: additional objects or none]*

attributes: interface, type of access

].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- *an operation is allowed according to ▸Table 6.6,*
- *[assignment: additional rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects or none]*

].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [

- *the GWA and SRV are not allowed to read meter data or the consumer log,*
- *the SRV must not be allowed to read, modify or delete any other TSF data not mentioned in ▸FDP_ACF.1.2,*
- *no external entity may access the TOE at an interface other than indicated in ▸Table 6.6,*
- *no external entity is allowed to read the shared secrets used for encryption except for the key exchange during usage of the key generation service*

].

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 fulfilled by ▸FDP_ACC.2

FMT_MSA.3 unfulfilled, see ▸Table 6.13: SFR Dependencies.

Application Note 41 The ST author shall consider the regulations from [BSI-TR-03109-1] for additional rules regarding the SMGW access SFP.

Application Note 42 Please be aware that the master key as well as the derived master key for the symmetric encryption via LMN also counts as “symmetric keys used for encryption”.

Subject	*Object*	*operation / type of access*	*interface*
authorized consumer	the version number of the TOE the SMGW time the status of time synchronization their own user data including their meter data and their consumer log the processing profiles associated with the consumer the certificates present on the TOE a list of the resources of the TOE available for the consumer	read access	HAN-CON or HAN-CLS
	management of the TSF according to ▸Table 6.7	operation and access as described in ▸Table 6.7	

Subject	*Object*	*operation / type of access*	*interface*
authorized SRV	the version number of the TOE the SMGW time the status of time synchronization the system log the calibration log the communication profiles the certificates present on the TOE the status of the interfaces of the TOE a list of the identified meters and the status of the connection to these a list of the identified CLS's and the status of the connection to these a list of the resources of the TOE available for the SRV	read access	HAN-CON or HAN-CLS
	management of the TSF according to ▸Table 6.7	operation and access as described in ▸Table 6.7	
authorized GWA	the version number of the TOE the SMGW time the status of time synchronization the system log the calibration log a list of the resources of the TOE available for the GWA	read access	WAN
	management of the TSF according to ▸Table 6.7	operation and access as described in ▸Table 6.7	
authorized meter	the SMGW time the meter config	read access	LMN
	management of the TSF according to ▸Table 6.7	operation and access as described in ▸Table 6.7	
authorized CLS	the version number of the TOE the SMGW time the status of time synchronization the processing profiles associated with the CLS the certificates present on the TOE the CLS's config the meter data associated with the CLS via a processing profile a list of the resources of the TOE available for that CLS	read access	HAN-CON or HAN-CLS
	management of the TSF according to ▸Table 6.7	operation and access as described in ▸Table 6.7	
unauthorized external entity	the SMGW time	read access	LMN, HAN-CON or HAN-CLS

Table 6.6 Rules for the SMGW access SFP

6.4.3 SMGW information flow SFP

6.4.3.1 FDP_IFC.2: Complete information flow control

FDP_IFC.2.1 The TSF shall enforce the [*SMGW information flow SFP*] on [*the TOE, the external entities GWA, SRV, CON, meter, CLS and external market participant, and all information flowing between them*] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 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.

Hierarchical to: FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 ▸directly fulfilled

6.4.3.2 FDP_IFF.1: Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [*SMGW information flow SFP*] based on the following types of subject and information security attributes: [

subjects: TOE, the external entities GWA, SRV, CON, meter, CLS and external market participant

information: any user data and TSF data that is sent to, from or via the TOE

attributes: interface, processing profile, communication profile, time

].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- *an information flow shall be permitted via a trusted channel as described in ▸FTP_PRO.1/TLS12 and [selection, choose one of: ▸FTP_PRO.1/TLS13 , none],*
- *an information flow via LMN shall be permitted via a trusted channel as described in ▸FTP_PRO.1/SYM,*
- *an information flow of meter data shall be according to the rules set in a corresponding processing profile,*
- *an information flow between the TOE and external entities shall be according to the rules set in a corresponding communication profile and processing profile,*
- *an information flow between CLS and external market participant shall be according to the rules set in a proxy communication profile*
- *[assignment: other rules or none]*

].

FDP_IFF.1.3 The TSF shall enforce the [*following rules:*

- *meter data received from meters shall be processed as defined in the corresponding processing profile,*
- *results of the processing of meter data shall be submitted to external market participants as defined in the processing profiles,*

].

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

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

- *information flow outside trusted channels shall be denied,*
- *the initiation of trusted channels by external entities in the WAN shall be denied,*
- *the TOE shall deny any acceptance of information by external entities unless they have been authorized,*
- *an information flow between the TOE and an external entity shall be denied if no corresponding communication profile exists*
- *an information flow between CLS and external market participant shall be denied if no corresponding proxy communication profile exists*
- *[assignment: rules based on security attributes that explicitly deny information flows]*

].

Hierarchical to: No other components.

Dependencies: FDP_IFC.1 fulfilled by ▸FDP_IFC.2

FMT_MSA.3 unfulfilled, see ▸Table 6.13: SFR Dependencies.

Application Note 43 Note that, according to O.SeparateIF, the TOE shall be designed with physically separated ports for WAN, LMN, HAN-CON and HAN-CLS.

Application Note 44 The assignment in ▸FDP_IFF.1.2 may be used by the ST author to specify additional rules (e.g. connections between devices in different HANs if the TOE is attached to more than one HAN) as long as those rules do not contradict the rest of the SFP.

Application Note 45 An information flow of meter data to an external market participant via the GWA is permitted if the parameters are set accordingly in the respective processing profile, see [BSI-TR-03109-1].

Application Note 46 The attribute "time" is necessary as the access to historical data is restricted to the validity period of the respective processing profile.

6.4.4 General requirements on user data protection

6.4.4.1 FDP_RIP.2: Full residual information protection

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [deallocation of the resource from] all objects.

Hierarchical to: FDP_RIP.1 Subset residual information protection

Dependencies: No dependencies.

Application Note 47 Please refer to [CC:2022] Part 2, Ch. F.11 for more detailed information about what kind of information this requirement applies to.

Please further note that this SFR has been used in order to ensure that information that is no longer used is made unavailable from a logical perspective. Specifically, it has to be ensured that this information is no longer available via an external interface (even if an access control or information flow policy would fail). However, this does not necessarily mean that the information is overwritten in a way that makes it impossible for an attacker to get access to it in case of having physical access to the memory of the TOE.

6.4.4.2 FDP_SDI.2: Stored data integrity monitoring and action

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for [assignment: *integrity errors*] on all objects, based on the following attributes: [assignment: *user data attributes*].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [assignment: *action to be taken*].

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

Dependencies: No dependencies.

Application Note 48 This PP defines that the TOE shall be capable of detecting integrity errors on all objects. This covers in particular the objects listed in [BSI-TR-03109-1]. The definition of real attributes that are used to implement this functionality are left to the ST author. Note that for the objects listed in [BSI-TR-03109-1], the TR further defines the actions to be taken in case of integrity errors.

Application Note 49 The developer should consider the use of the built-in security module as an anchor of trust for this functionality.

6.5 Class FIA: Identification and authentication

6.5.1 Overview

The TOE requires the identification and authentication of an external entity before any other TSF-mediated action can take place on behalf of that entity. The SFRs in this section model the necessary functionality of the TOE.

6.5.2 FIA_AFL.1: Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [~~**an administrator**~~**a GWA** configurable positive integer within [*3 and 10*]] unsuccessful authentication attempts occur related to [*password-based authentication attempts by the consumer*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [assignment: *list of actions*].

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 ▸directly fulfilled

Application Note 50 The actions of the TSF in ▸FIA_AFL.1.2 shall be in such a way that the functionality to authenticate for SRVs and CLS is not affected.

6.5.3 FIA_ATD.1: User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

- *user identity*
- *status of identity (authenticated or not)*
- *connecting network (WAN, HAN or LMN)*
- *role membership*
- *[assignment: list of security attributes or none]*

].

Hierarchical to: No other components.

Dependencies: No dependencies.

6.5.4 FIA_UAU.1: Timing of authentication

FIA_UAU.1.1 The TSF shall allow [*read access to the SMGW time*] on behalf of ~~**the user**~~**external entities in the HAN and LMN** to be performed before ~~**the user is**~~**external entities in the HAN and LMN are** authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Hierarchical to: No other components.

Dependencies: FIA_UID.1 ▸directly fulfilled

Application Note 51 Please refer to [BSI-TR-03109-1] for a more detailed overview on the authentication of the TOE users.

6.5.5 FIA_UAU.5: Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide [

- *password-based authentication*
- *authentication via pre-shared keys as described in ▸FTP_PRO.2/SYM*
- *authentication via signature of a wake-up call as described in [BSI-TR-03109-1]*
- *certificate-based authentication for TLS as described in ▸FTP_PRO.2/TLS12 and [selection, choose one of: ▸FTP_PRO.2/TLS13 , none]*
- *[assignment: additional authentication mechanisms for CON]*

] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the **rules**[

- *password-based authentication or certificate-based authentication [selection, choose one of: [assignment: additional authentication mechanisms for CON] , no additional authentication mechanism] shall be used for the authentication of CON at HAN-CON or HAN-CLS*
- *certificate-based authentication shall be used for the authentication of*
  - *GWA at WAN,*
  - *SRV at HAN-CON or HAN-CLS,*
  - *bidirectionally connected meter at LMN,*
  - *CLS at HAN-CON or HAN-CLS,*
  - *external market participant at WAN*
- *pre-shared keys shall be used for the authentication of a meter at LMN*

].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 52 Please refer to [BSI-TR-03109-1] for a more detailed overview on the authentication of the TOE users.

Application Note 53 Note that in the case of usage of authentication via passwords, the password shall not be stored in plain text. A cryptographic hash as described in [BSI-TR-03109-1] shall be used.

6.5.6 FIA_UID.1: Timing of identification

FIA_UID.1.1 The TSF shall allow [assignment: *read access to the SMGW time*] on behalf of ~~**the user**~~ **external entities in the HAN and LMN** to be performed before ~~the user is~~ **external entities in the HAN and LMN are** identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any TSF-mediated actions on behalf of that user.

Hierarchical to: No other components.

Dependencies: No dependencies.

6.5.7 FIA_USB.1: User-subject binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [*attributes as defined in ▸FIA_ATD.1*].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: *rules for the initial association of attributes*].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *rules for the changing of attributes*].

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 ▸directly fulfilled

6.6 Class FMT: Security management

6.6.1 Overview

This section covers the management of the TSF.

6.6.2 FMT_MOF.1: Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [modify the behaviour of] the functions [*for management as defined in ▸FMT_SMF.1*] to [*roles and restrictions as defined in ▸Table 3.1 and ▸Table 6.7*].

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 ▸directly fulfilled

FMT_SMF.1 ▸directly fulfilled

Function	*Limitation*
Management of profiles	The authorized GWA is allowed to read and write the processing profiles and the communication profiles.
Management of tarifing event data	The authorized GWA is allowed to read and write tarifing event data for a processing profile. Authorized CLS associated with a processing profile are allowed to read and write tarifing event data for that processing profile.
WAN communication parameters	Authorized GWAs and SRVs are allowed to read and write WAN communication parameters as well as the WAN interface configuration.
TOE reset	The authorized GWA and authorized SRVs are allowed to execute the reset functionality of the TOE, rendering • communication profiles for CLS, CON, LMN, external market participants and proxy communication profiles • processing profiles • meter data • system log data • consumer log data • calibration log data except for events logging successful firmware updates of the TOE • further personally identifiable information (PII) irreversibly inaccessible.

Function	*Limitation*
Wake-up call	The authorized GWA is allowed to execute the establishment of a wake-up call to the TOE.
Pairing of a meter	The authorized GWA is allowed to execute the initiation of a pairing of the SMGW with a meter.
TLS proxy channel establishment	Authorized CLS are allowed to execute the request of a TLS proxy channel establishment to an external market participant. The authorized GWA is allowed to execute the request of a TLS proxy channel establishment between a CLS and an external market participant.
Hash of the consumer password	The authorized GWA and the authorized consumer are allowed to change the password of the respective consumer, i.e., they have write access to the hash of the consumer password. Note that the password shall not be stored in plain text.
Management of CLS config	The authorized GWA is allowed to read and write the CLS config.
Management of meter config	The authorized GWA and authorized SRV are allowed to read the meter config. The authorized GWA is allowed to write the meter config.
Public-private key pair and certificate generation and distribution	Authorized CLS and authorized meters are allowed to execute the request for the generation and distribution of a public-private key pair and the corresponding self-signed certificate.
Self-test	The authorized GWA and authorized SRVs are allowed to execute the self-test functionality of the TOE as described in ▸FPT_TST.1.
Firmware update	The authorized GWA is allowed to execute the initiation of a firmware update. The firmware update must only be possible after the authenticity of the firmware update has been verified (using the services of the security module and the trust anchor of the SMGW developer) and if the version number of the new firmware is higher than the version of the installed firmware.
Restart of the TOE	The authorized GWA and authorized SRVs are allowed to execute the initiation of a restart of the TOE.
All other management functions as defined in ▸FMT_SMF.1	The authorized GWA is allowed to access and execute all management functions as defined in ▸FMT_SMF.1 that were not mentioned or included in the rows above.

Table 6.7 Restrictions on management functions

Application Note 54: For details concerning the WAN communication parameters that may be altered by an authorized SRV see [BSI-TR-03109-1].

Application Note 55: The deletion of the calibration log by the GWA or SRV is intended to be used prior to a de-installation of the TOE. It has to be ensured by the GWA/the SRV, that the deletion of the calibration audit trail happens only after a successful export of this data. See also [BSI-TR-03109-1].

6.6.3 FMT_MTD.1: Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [delete] the [*audit data in the calibration audit trail except for [assignment: events that shall remain on the TOE according to [BSI-TR-03109-1]]*] to [*the authorized GWA, the authorized SRV*].

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 ▸directly fulfilled

FMT_SMF.1 ▸directly fulfilled

Application Note 56 This functionality has to be used by the GWA or the SRV prior to a de-installation of the TOE. It has to be ensured by the GWA/the SRV that the deletion of the calibration audit trail happens only after a successful export of this data. See also [BSI-TR-03109-1].

6.6.4 FMT_SMF.1: Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*list of management functions as defined in* ▸*Table 6.8 and in the left column of* ▸*Table 6.7 and [assignment: additional functionalities]*].

Hierarchical to: No other components.

Dependencies: No dependencies.

SFR	Management functionality
▸FAU_ARP.1/SYS	• The management (addition, removal, or modification) of actions.
▸FAU_GEN.1/SYS ▸FAU_GEN.1/CON ▸FAU_GEN.1/CAL	-
▸FAU_SAA.1/SYS	• Maintenance of the rules by (adding, modifying, deletion) of rules from the set of rules.
▸FAU_SAR.1/SYS ▸FAU_SAR.1/CON ▸FAU_SAR.1/CAL	-
▸FAU_STG.5/SYS ▸FAU_STG.5/CON	• Maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure. • Size configuration of the audit trail that is available before the oldest events get overwritten (as long as potential security violations can be detected).
▸FAU_STG.5/CAL	• Maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.
▸FAU_GEN.2	-
▸FAU_STG.3	• Maintenance of the parameters that control the audit storage capability for the consumer log and the system log.
▸FCS_CKM.1/SERVICE	• Management of key material. • Management of key material stored in the security module. • Management of key material brought into the gateway during the pairing process with meters.
▸FCS_CKM.5/TLS	
▸FCS_CKM.5/CMAC	
▸FCS_CKM.5/X963	
▸FCS_COP.1/AES	
▸FCS_COP.1/HMAC	
▸FCS_COP.1/MTRCMAC	
▸FCS_COP.1/AESWRAP	
▸FCS_COP.1/HASH	-
▸FCS_COP.1/MEM	• Management of key material.
▸FCS_CKM.6	-
▸FDP_ACC.2	-
▸FDP_ACF.1	-
▸FDP_IFC.2	-

SFR	Management functionality
▸FDP_IFF.1	• Managing the attributes used to make explicit access based decisions. • Add authorized units for communication (pairing). • Management of endpoint to be contacted after successful wake-up call. • Management of communication profiles. • Managing the attributes in processing profiles specified in [BSI-TR-03109-1] used to make explicit access based decisions.
▸FDP_RIP.2	-
▸FDP_SDI.2	-
▸FIA_AFL.1	• Management of the threshold for unsuccessful authentication attempts.
▸FIA_ATD.1	-
▸FIA_UAU.1	• Management of the authentication data by an authorized GWA. • Management of their own password as authentication data by the respective authorized consumer.
▸FIA_UAU.5	-
▸FIA_UID.1	• The management of the user identities.
▸FIA_USB.1	-
▸FMT_MOF.1	-
▸FMT_MTD.1	-
▸FMT_SMF.1	-
▸FMT_SMR.1	• Managing the group of users that are part of a role.
▸FPR_CON.1	• Definition of the interval in FPR_CON.1.2 if definable within the operational phase of the TOE.
▸FPR_PSE.1	-
▸FPT_FLS.1	-
▸FPT_PHP.1	-
▸FPT_RPL.1	-
▸FPT_STM.1	• Management of a time source.
▸FPT_STM.2	• Management of a time source.
▸FPT_TST.1	-
▸FTP_PRO.1/TLS12	-
▸FTP_PRO.2/TLS12	
▸FTP_PRO.3/TLS12	
▸FTP_PRO.1/TLS13 (optional)	-
▸FTP_PRO.2/TLS13 (optional)	
▸FTP_PRO.3/TLS13 (optional)	
▸FTP_PRO.1/SYM	-
▸FTP_PRO.2/SYM	
▸FTP_PRO.3/SYM	
▸FTP_PRO.1/CMS	-
▸FTP_PRO.2/CMS	

SFR	Management functionality
▸FTP_PRO.3/CMS	

Table 6.8 SFR related management functionalities

6.6.5 FMT_SMR.1: Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [

authorized consumer,

authorized GWA,

authorized SRV,

authorized CLS,

authorized external market participant,

[assignment: the authorized identified roles].

].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Hierarchical to: No other components.

Dependencies: FIA_UID.1 ▸directly fulfilled

Application Note 57 The roles "authorized GWA", "authorized SRV", "authorized consumer", "authorized CLS" and "authorized external market participant" are the roles that are needed for the operation of the TOE. However, the assignment in ▸FMT_SMR.1.1 deliberately allows the definition of additional roles. The ST author is asked to complete the roles that are required for a specific TOE and introduce a more complex set of roles, if necessary.

6.7 Class FPR: Privacy

6.7.1 FPR_CON.1: Communication concealing

FPR_CON.1.1 The TSF shall enforce the [*SMGW information flow SFP*] in order to ensure that no personally identifiable information (PII) can be obtained by an analysis of [assignment: *characteristics of the information flow that need to be concealed*].

FPR_CON.1.2 The TSF shall connect to [assignment: *list of external entities*] in intervals as follows [selection, choose one of: *weekly, daily, hourly, [assignment: other interval]*] to conceal the data flow.

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 58 The interval and the list of external entities that shall be used in FPR_CON.1.2 highly depends on the actual application case. Therefore, the assignments in FPR_CON.1.2 are left to the ST author.

Application Note 59 Please note, that concealing shall be used accordingly to the description of O.ConcealWAN (cmp. ▸Section 4.1) and shall be applied to all privacy-relevant information[23]

[23] Privacy-relevant data in this case includes at least all consumption and feed data that could be mapped to a specific user or user group

6.7.2 FPR_PSE.1: Pseudonymity

FPR_PSE.1.1 The TSF shall ensure that [assignment: *set of users and/or subjects*] are unable to determine the real user name bound to [assignment: *list of subjects and/or operations and/or objects*].

FPR_PSE.1.2 The TSF shall be able to provide [assignment: *number of aliases*] aliases of the real user name to [assignment: *list of subjects*].

FPR_PSE.1.3 The TSF shall [selection, choose one of: *determine an alias for a user, accept the alias from the user*] and verify that it conforms to the [assignment: *alias metric*].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 60 When the TOE submits information about the consumption or production of a certain commodity that is not relevant for the billing process nor for a secure operation of the smart grid, there might be no need that this information is sent with PII. In those cases the TOE shall replace every PII by a pseudonymous identifier if configured by the GWA within the corresponding processing profile. This has to be modelled by the ST author according to national regulations. See also [BSI-TR-03109-1].

6.8 Class FPT: Protection of the TSF

6.8.1 FPT_FLS.1: Failure with preservation of secure state

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

all types of failures in the TSF listed in ▸Table 6.9,

[assignment: other types of failures in the TSF]

].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 61 The local clock shall be as exact as required by normative or legislative regulations. For more information, see [BSI-TR-03109-1].

Application Note 62 If necessary, the ST author shall expand ▸Table 6.9 to add other types of failures in the TSF according to the assignment in the SFR and mark them as an assignment accordingly. In particular, the failure of a test in ▸FDP_SDI.2 or ▸FPT_TST.1 and the reaction of the TOE shall be described.

Type of failure	*Reaction of the TSF*
Attempts to synchronize the SMGW time have failed for too long, cf. [BSI-TR-03109-1].	The TSF shall • ensure that any following meter data is not used, • reversibly stop operation, • inform the GWA.
The calibration log is full.	

Table 6.9 Types of failures and reaction of the TSF

6.8.2 FPT_PHP.1: Passive detection of physical attack

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that can compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 63 A passive detection of a physical attack is classically achieved by a seal and an appropriate physical design of the TOE that allows the consumer (or any other party) to verify the physical integrity of the SMGW and by that of the TOE.

6.8.3 FPT_RPL.1: Replay detection

FPT_RPL.1.1 The TSF shall detect replay for the following entities: [*wake-up messages sent by the GWA according to [BSI-TR-03109-1], messages sent by unidirectionally communicating meters in LMN*].

FPT_RPL.1.2 The TSF shall perform [*ignore replayed data*] when replay is detected.

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 64 Note that for messages sent via TLS, replay detection is built-in, see also ▸FTP_PRO.3/TLS12 and optionally ▸FTP_PRO.3/TLS13.

6.8.4 FPT_STM.1: Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps. **Time stamps are considered reliable if the internal system time is synchronized with the reliable external time source according to [BSI-TR-03109-1].**

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 65 If the deviation between the SMGW time and the remote time is acceptable, the SMGW time shall be updated according to the remote time. If the deviation is not acceptable, the TOE shall proceed as described in ▸FPT_FLS.1.

There are several ways to achieve the reliability of the external source. On the one hand there may be a source in the WAN that has an acceptable reliability on its own (e.g. because it is operated by a very trustworthy organization (an official legal time issued by the calibration authority would be a good example for such a source)). On the other hand a developer may choose to maintain multiple external sources that all have a certain level of reliability but no absolute reliability. When using such sources the TOE shall contact more than one source and harmonize the results in order to ensure that no attack happened.

6.8.5 FPT_STM.2: Time source

FPT_STM.2.1 The TSF shall allow the [*authorized GWA*] to [*configure another time source*].

Hierarchical to: No other components.

Dependencies: FPT_STM.1 ▸directly fulfilled

FMT_SMR.1 ▸directly fulfilled

Application Note 66 The time stamps as defined by ▸FPT_STM.1 shall be of sufficient exactness. Therefore, the SMGW time is synchronized regularly with a reliable external time source configured by the GWA. Radio controlled clocks shall not be used. However, the TOE's local clock also needs a sufficient exactness as the synchronization will fail if the deviation is too large. In addition, if attempts to synchronize the time have failed for too long, the following meter data shall not be used (the TOE has to preserve a secure state according to ▸FPT_FLS.1). Therefore, the TOE's local clock shall be as exact as required by normative or legislative regulations. For more information, see [BSI-TR-03109-1].

Please be aware, that in case of initial connection establishments to the GWA for NTP purposes or after leaving reversible secure state modes, the temporal TLS certificate validity check may me skipped.

6.8.6 FPT_TST.1: TSF self-testing

FPT_TST.1.1 The TSF shall run a suite of the following self-tests [during initial start-up, periodically during normal operation, "at the request of **~~the authorized user~~the authorized GWA, the authorized SRV**"] to demonstrate the correct operation of [the TSF]: [assignment: *list of self-tests run by the TSF*].

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of [TSF data].

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of [TSF].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 67 The self-test suite as defined in ▸FPT_TST.1 shall contain at least a test to verify the integrity of the TOE firmware as well as tests to verify the correct function of cryptographic operations, including reachability and correct operation of the security module. Please note that [BSI-TR-03109-1] includes further requirements on the self-test functionality of the SMGW.

6.9 Class FTP: Trusted path/channels

6.9.1 Trusted channel protocol using TLS v1.2

6.9.1.1 FTP_PRO.1/TLS12: Trusted channel protocol for TLSv1.2

FTP_PRO.1.1/TLS12 The TSF shall implement [*TLS version 1.2*] acting as [*defined protocol role as in* ▸*Table 6.10*] in accordance with: [*[RFC5246]*].

FTP_PRO.1.2/TLS12 The TSF shall enforce usage of the trusted channel for [*communication at the interfaces as in* ▸*Table 6.10 with the respective roles as in* ▸*Table 6.10*] in accordance with: [*[BSI-TR-03109-1]*].

FTP_PRO.1.3/TLS12 The TSF shall permit [itself, its peer] **as depicted in** ▸**Table 6.10** to initiate communication via the trusted channel.

FTP_PRO.1.4/TLS12 The TSF shall enforce the following rules for the trusted channel: [*none*].

FTP_PRO.1.5/TLS12 The TSF shall enforce the following static protocol options: [

- *The TOE shall close TLS sessions to external entities after 48 hours.*
- *The TOE shall close TLS sessions to CON and SRV after 10 minutes of inactivity.*

].

FTP_PRO.1.6/TLS12 The TSF shall negotiate one of the following protocol configurations with its peer: [

- *One of the following cipher suites:*
  - *[selection: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384] according to [RFC5289].*
- *One of the following curve parameters:*

  - *[selection: secp256r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1, secp384r1] according to [RFC7027] respectively [RFC8422].*
- *The following signature algorithm: ECDSA.*
- *One of the following hash algorithms, modelled according to* ▸*FCS_COP.1/HASH:*
  - *[selection: SHA-256, SHA-384, SHA-512].*
- *The TOE shall not support session renegotiation.*
- *The TOE shall use the Supported Point Formats Extension according to [RFC8422].*
- *The TOE shall not support truncated HMAC.*
- *As a TLS-client, the TOE shall offer encrypt-then-MAC in the client-hello according to [RFC7366].*
- *As a TLS-server, the TOE shall either choose a GCM cipher suite or use encrypt-then-MAC in the server-hello according to [RFC7366].*

].

Hierarchical to: No other components.

Dependencies: FTP_PRO.2 fulfilled by ▸FTP_PRO.2/TLS12

FTP_PRO.3 fulfilled by ▸FTP_PRO.3/TLS12

Application Note 68 The ST author shall complete the selection operations in accordance with [BSI-TR-03109-3], taking into account [BSI-TR-03109-1]. In particular, cipher suites, curve parameters and hash algorithms that are mandatory according to [BSI-TR-03109-3] shall be selected.

Application Note 69 Please note that the requirement on a trusted channel for the consumer interface is implicitly fulfilled for the case that the user interface is implemented via a local display at the TOE.

Interface	Peer user role	TOE protocol role	Initiator of communication
WAN	GWA	client	itself
WAN	External market participant	client	itself
LMN	Bidirectionally connected meters	client	itself
HAN-CON / HAN-CLS	CLS	client, server	itself, its peer
HAN-CON / HAN-CLS	SRV	server	its peer
HAN-CON / HAN-CLS	CON	server	its peer

Table 6.10 Interfaces and roles for trusted channel

6.9.1.2 FTP_PRO.2/TLS12: Trusted channel establishment for TLSv1.2

FTP_PRO.2.1/TLS12 The TSF shall establish a shared secret with ~~its peer~~**the GWA, external market participant, bidirectionally connected meter, CLS, service technician and consumer** using one of the following mechanisms: [*ECKA-DH*].

FTP_PRO.2.2/TLS12 The TSF shall authenticate [its peer, itself to its peer] using one of the following mechanisms: [

- *ECDSA with all its peers according to [BSI-TR-03111]*
- *For the consumer, as an alternative option, the TSF shall be able to authenticate the consumer using passwords.*
- *To access the asset SMGW time, the TSF may omit the authentication of external entities in the HAN and LMN.*

] and according to the following rules: [*[BSI-TR-03109-1], [BSI-TR-03109-3]*].

FTP_PRO.2.3/TLS12 The TSF shall use [*the PRF as in ▸FCS_CKM.5/TLS*] to derive the following cryptographic keys from a shared secret: [*client and server write MAC and encryption keys*].

Hierarchical to: No other components.

Dependencies: FTP_PRO.1 fulfilled by ▸FTP_PRO.1/TLS12

[FCS_CKM.1 unfulfilled, see ▸Table 6.13: SFR Dependencies. or

FCS_CKM.2]

FCS_CKM.5 fulfilled by ▸FCS_CKM.5/TLS

FCS_COP.1 unfulfilled, see ▸Table 6.13: SFR Dependencies.

Application Note 70 Note that for ECKA-DH in ▸FTP_PRO.2.1/TLS12 and for ECDSA in ▸FTP_PRO.2.2/TLS12, the services of the security module shall be used.

6.9.1.3 FTP_PRO.3/TLS12: Trusted channel data protection for TLSv1.2

FTP_PRO.3.1/TLS12 The TSF shall protect data in transit from unauthorised disclosure using one of the following mechanisms: [*AES in CBC-mode and GCM-mode according to ▸FCS_COP.1/AES*].

FTP_PRO.3.2/TLS12 The TSF shall protect data in transit from [modification, deletion, insertion, replay] using one of the following mechanisms: [*AES in GCM-mode according to ▸FCS_COP.1/AES, HMAC according to ▸FCS_COP.1/HMAC*].

Hierarchical to: No other components.

Dependencies: FTP_PRO.1 fulfilled by ▸FTP_PRO.1/TLS12

FTP_PRO.2 fulfilled by ▸FTP_PRO.2/TLS12

FCS_COP.1 fulfilled by ▸FCS_COP.1/AES and ▸FCS_COP.1/HMAC

Application Note 71: If the TOE additionally supports TLS in version 1.3, the ST author shall iterate FTP_PRO using the set of SFRs described in ▸Section 6.9.4.

6.9.2 Trusted channel protocol for symmetric-encryption-based communication

6.9.2.1 FTP_PRO.1/SYM: Trusted channel protocol for unidirectional communication with meters in LMN

FTP_PRO.1.1/SYM The TSF shall implement [*wM-BUS*] acting as [*server*] in accordance with: [*[EN13757-4]*].

FTP_PRO.1.2/SYM The TSF shall enforce usage of the trusted channel for [*all unidirectional communication with meters in LMN*] in accordance with: [*[EN13757-4], [EN13757-7], [BSI-TR-03109-3]*].

FTP_PRO.1.3/SYM The TSF shall permit [its peer] to initiate communication via the trusted channel.

FTP_PRO.1.4/SYM The TSF shall enforce the following rules for the trusted channel: [*none*].

FTP_PRO.1.5/SYM The TSF shall enforce the following static protocol options: [*security mode 7 using AES-CBC-128 as modelled in ▸FCS_COP.1/AES, [selection, choose one of: security mode 10 using AES-CCM-128 as modelled in ▸FCS_COP.1/AES , none]*].

FTP_PRO.1.6/SYM The TSF shall negotiate one of the following protocol configurations with its peer: [*none*].

Hierarchical to: No other components.

Dependencies: FTP_PRO.2 fulfilled by ▸FTP_PRO.2/SYM

FTP_PRO.3 fulfilled by ▸FTP_PRO.3/SYM

6.9.2.2 FTP_PRO.2/SYM: Trusted channel establishment for unidirectional communication with meters in LMN

FTP_PRO.2.1/SYM The TSF shall establish a shared secret with ~~its peer~~**unidirectionally communicating meters in LMN** using one of the following mechanisms: [

- *the shared key is brought into the TOE by the GWA*
- *AES-CMAC according to ▸FCS_CKM.5/CMAC*

].

FTP_PRO.2.2/SYM The TSF shall authenticate [its peer] using one of the following mechanisms: [*AES-CMAC according to ▸FCS_COP.1/MTRCMAC*] and according to the following rules: [*[BSI-TR-03109-1], [BSI-TR-03109-3]*].

FTP_PRO.2.3/SYM The TSF shall use [*AES-CMAC according to ▸FCS_CKM.5/CMAC*] to derive the following cryptographic keys from a shared secret: [*K_{Enc}, K_{MAC}, [selection, choose one of: "L_{Enc}, L_{MAC}", none]*].

Hierarchical to: No other components.

Dependencies: FTP_PRO.1 fulfilled by ▸FTP_PRO.1/SYM

[FCS_CKM.1 or

FCS_CKM.2 unfulfilled, see ▸Table 6.13: SFR Dependencies.]

FCS_CKM.5 fulfilled by ▸FCS_CKM.5/CMAC

FCS_COP.1 fulfilled by ▸FCS_COP.1/MTRCMAC

6.9.2.3 FTP_PRO.3/SYM: Trusted channel data protection for unidirectional communication with meters in LMN

FTP_PRO.3.1/SYM The TSF shall protect data in transit from unauthorised disclosure using one of the following mechanisms: [*AES-CBC-128 according to ▸FCS_COP.1/AES, [selection, choose one of: AES-CCM-128 according to ▸FCS_COP.1/AES, none]*].

FTP_PRO.3.2/SYM The TSF shall protect data in transit from [modification, insertion, replay] using one of the following mechanisms: [*AES-CMAC according to ▸FCS_COP.1/MTRCMAC, [selection, choose one of: AES-CCM-128 according to ▸FCS_COP.1/AES, none]*].

Hierarchical to: No other components.

Dependencies: FTP_PRO.1 fulfilled by ▸FTP_PRO.1/SYM

FTP_PRO.2 fulfilled by ▸FTP_PRO.2/SYM

FCS_COP.1 fulfilled by ▸FCS_COP.1/AES and ▸FCS_COP.1/MTRCMAC

Application Note 72 The ST author shall complete the selection operations in accordance with [BSI-TR-03109-3], taking into account [BSI-TR-03109-1].

6.9.3 Trusted channel protocol for content data encryption

6.9.3.1 FTP_PRO.1/CMS: Trusted channel protocol for content data encryption

FTP_PRO.1.1/CMS The TSF shall implement [*CMS*] acting as [*content encrypting entity, [selection: content decrypting entity, none]*] in accordance with: [*[RFC5652], [RFC5083], [RFC5084]*].

FTP_PRO.1.2/CMS The TSF shall enforce usage of ~~the trusted channel~~**CMS** for [*authenticated encryption and signing of data for data sent to an external market participant via the GWA*] in accordance with: [*[BSI-TR-03109-1]*].

FTP_PRO.1.3/CMS The TSF shall permit [itself, its peer] to ~~initiate communication via the trusted channel~~**use CMS for authenticated encryption and signing of data**.

FTP_PRO.1.4/CMS The TSF shall enforce the following rules for the trusted channel: [*none*].

FTP_PRO.1.5/CMS The TSF shall enforce the following static protocol options: [*none*].

FTP_PRO.1.6/CMS The TSF shall negotiate one of the following protocol configurations with its peer: [*none*].

Hierarchical to: No other components.

Dependencies: FTP_PRO.2 fulfilled by ▸FTP_PRO.2/CMS

FTP_PRO.3 fulfilled by ▸FTP_PRO.3/CMS

Application Note 73 It is not required that the TOE offers content data decryption. If it provides such cryptographic functionality, the ST author shall select this accordingly.

6.9.3.2 FTP_PRO.2/CMS: Trusted channel establishment for content data encryption

FTP_PRO.2.1/CMS The TSF shall establish a shared secret with its peer using one of the following mechanisms: [*ECKA-EG provided by the security module and X9.63 as key derivation function according to ▸FCS_CKM.5/X963*].

FTP_PRO.2.2/CMS The TSF shall authenticate [its peer, itself to its peer] using one of the following mechanisms: [*ECDSA*] and according to the following rules: [*[BSI-TR-03109-1], [BSI-TR-03109-3]*].

FTP_PRO.2.3/CMS The TSF shall use [*X9.63 according to ▸FCS_CKM.5/X963*] to derive the following cryptographic keys from a shared secret: [*key wrapping key for CMS*].

Hierarchical to: No other components.

Dependencies: FTP_PRO.1 fulfilled by ▸FTP_PRO.1/CMS

[FCS_CKM.1 unfulfilled, see ▸Table 6.13: SFR Dependencies. or

FCS_CKM.2]

FCS_CKM.5 fulfilled by ▸FCS_CKM.5/X963

FCS_COP.1 fulfilled by ▸FCS_COP.1/AESWRAP

Application Note 74 Note that for ECKA-EG in ▸FTP_PRO.2.1/CMS and for ECDSA in ▸FTP_PRO.2.2/CMS, the services of the security module shall be used.

6.9.3.3 FTP_PRO.3/CMS: Trusted channel data protection for content data encryption

FTP_PRO.3.1/CMS The TSF shall protect data in transit from unauthorised disclosure using one of the following mechanisms: [*AES-GCM or AES-CBC according to ▸FCS_COP.1/AES*].

FTP_PRO.3.2/CMS The TSF shall protect data in transit from [modification, deletion, insertion, replay] using one of the following mechanisms: [*AES-GCM or AES-CMAC according to ▸FCS_COP.1/AES or ▸FCS_COP.1/CMSCMAC, and ECDSA provided by the security module*].

Hierarchical to: No other components.

Dependencies: FTP_PRO.1 fulfilled by ▸FTP_PRO.1/CMS

FTP_PRO.2 fulfilled by ▸FTP_PRO.2/CMS

FCS_COP.1 fulfilled by ▸FCS_COP.1/AES and ▸FCS_COP.1/CMSCMAC

6.9.4 Trusted channel protocol using TLS v1.3 (optional SFRs)

Application Note 75: This section contains a set of SFRs for the implementation of TLS v1.3. If TLS v1.3 is implemented in the TOE, this set of SFRs shall be included in the ST and the operations have to be fulfilled as required.

6.9.4.1 FTP_PRO.1/TLS13: Trusted channel protocol for TLSv1.3 (optional)

FTP_PRO.1.1/TLS13 The TSF shall implement [*TLS version 1.3*] acting as [*defined protocol role as in* ▸*Table 6.10*] in accordance with: [*[RFC8446] and [BSI-TR-03109-3]*].

FTP_PRO.1.2/TLS13 The TSF shall enforce usage of the trusted channel for [*communication at the interfaces as in* ▸*Table 6.10 with the respective roles as in* ▸*Table 6.10*] in accordance with: [*[BSI-TR-03109-1], [BSI-TR-03109-3]*].

FTP_PRO.1.3/TLS13 The TSF shall permit [itself, its peer] **as depicted in** ▸**Table 6.10** to initiate communication via the trusted channel.

FTP_PRO.1.4/TLS13 The TSF shall enforce the following rules for the trusted channel: [*none*].

FTP_PRO.1.5/TLS13 The TSF shall enforce the following static protocol options: [

- *The TOE shall close TLS sessions to external entities after 48 hours.*
- *The TOE shall close TLS sessions to CON and SRV after 10 minutes of inactivity.*

].

FTP_PRO.1.6/TLS13 The TSF shall negotiate one of the following protocol configurations with its peer: [

- *One of the following cipher suites:*
  - *[selection: TLS_AES_128_GCM_SHA256 , TLS_AES_256_GCM_SHA384 , TLS_AES_128_CCM_SHA256] according to [RFC8422].*
- *One of the following curve parameters:*
  - *[selection: brainpoolP256r1tls13, brainpoolP384r1tls13, secp256r1, brainpoolP512r1tls13, secp384r1] according to [RFC8422] respectively [RFC8734].*
- *The TOE shall use the signature algorithm extension according to [RFC8446].*
- *One of the following signature algorithms for the verification of server signatures: [selection: ecdsa_brainpoolP256r1tls13_sha256, ecdsa_brainpoolP384r1tls13_sha384, ecdsa_brainpoolP512r1tls13_sha512, ecdsa_secp256r1_sha256, ecdsa_secp384r1_sha384] according to [RFC8446] respectively [RFC8734].*
- *One of the following signature algorithms for the verification of certificates: [selection: ecdsa_brainpoolP256r1tls13_sha256, ecdsa_brainpoolP384r1tls13_sha384, ecdsa_brainpoolP512r1tls13_sha512].*
- *One of the following handshake modes [selection: ECDHE, PSK with ECDHE].*
- *The TOE shall not support sending or receiving 0-RTT data.*

].

Hierarchical to: No other components.

Dependencies: FTP_PRO.2 fulfilled by ▸FTP_PRO.2/TLS13

FTP_PRO.3 fulfilled by ▸FTP_PRO.3/TLS13

Application Note 76 The ST author shall complete the selection operations in accordance with [BSI-TR-03109-3], taking into account [BSI-TR-03109-1]. In particular, cipher suites, curve parameters and hash algorithms that are mandatory according to [BSI-TR-03109-3] shall be selected.

Application Note 77 Please note that the requirement on a trusted channel for the consumer interface is implicitly fulfilled for the case that the user interface is implemented via a local display at the TOE.

6.9.4.2 FTP_PRO.2/TLS13: Trusted channel establishment for TLSv1.3 (optional)

FTP_PRO.2.1/TLS13 The TSF shall establish a shared secret with ~~its peer~~**the GWA, external market participant, bidirectionally connected meter, CLS, service technician and consumer** using one of the following mechanisms: [*[selection: ECDHE, PSK with ECDHE]*].

FTP_PRO.2.2/TLS13 The TSF shall authenticate [its peer, itself to its peer] using one of the following mechanisms: [

- *ECDSA with all its peers according to [BSI-TR-03111]*
- *For the consumer, as an alternative option, the TSF shall be able to authenticate the consumer using passwords.*
- *To access the asset SMGW time, the TSF may omit the authentication of external entities in the HAN and LMN.*

] and according to the following rules: [*[BSI-TR-03109-1], [BSI-TR-03109-3]*].

FTP_PRO.2.3/TLS13 The TSF shall use [*the HKDF as in ▸FCS_CKM.5/TLS*] to derive the following cryptographic keys from a shared secret: [*client and server write MAC and encryption keys*].

Hierarchical to: No other components.

Dependencies: FTP_PRO.1 fulfilled by ▸FTP_PRO.1/TLS13

[FCS_CKM.1 unfulfilled, see ▸Table 6.13: SFR Dependencies. or

FCS_CKM.2]

FCS_CKM.5 fulfilled by ▸FCS_CKM.5/TLS

FCS_COP.1 unfulfilled, see ▸Table 6.13: SFR Dependencies.

Application Note 78 The ST author shall complete the selection operations in accordance with [BSI-TR-03109-3], taking into account [BSI-TR-03109-1].

Application Note 79 Note that for ECDHE in ▸FTP_PRO.2.1/TLS13 and for ECDSA in ▸FTP_PRO.2.2/TLS13, the services of the security module shall be used.

6.9.4.3 FTP_PRO.3/TLS13: Trusted channel data protection for TLSv1.3 (optional)

FTP_PRO.3.1/TLS13 The TSF shall protect data in transit from unauthorised disclosure using one of the following mechanisms: [*AES in GCM-mode and CCM-mode according to ▸FCS_COP.1/AES*].

FTP_PRO.3.2/TLS13 The TSF shall protect data in transit from [modification, deletion, insertion, replay] using one of the following mechanisms: [*AES in GCM-mode and CCM-mode according to ▸FCS_COP.1/AES*].

Hierarchical to: No other components.

Dependencies: FTP_PRO.1 fulfilled by ▸FTP_PRO.1/TLS13

FTP_PRO.2 fulfilled by ▸FTP_PRO.2/TLS13

FCS_COP.1 fulfilled by ▸FCS_COP.1/AES

6.10 Security assurance requirements for the TOE

The minimum evaluation assurance level for this PP is **EAL 4 augmented by AVA_VAN.5 and ALC_FLR.2**.

The following table lists the assurance components which are therefore applicable to this PP.

Assurance class	Assurance component
Development	ADV_ARC.1
	ADV_FSP.4
	ADV_IMP.1

Assurance class	Assurance component
	ADV_TDS.3
Guidance documents	AGD_OPE.1
	AGD_PRE.1
Life-cycle support	ALC_CMC.4
	ALC_CMS.4
	ALC_DEL.1
	ALC_DVS.1
	ALC_LCD.1
	ALC_TAT.1
	ALC_FLR.2
Security target evaluation	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
Tests	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
Vulnerability assessment	AVA_VAN.5

Table 6.11 Security assurance requirements

6.10.1 Refinements of security assurance requirements

In the following, several refinements to the existing CC security assurance requirements are listed, which shall be applied during the corresponding development and evaluation process:

- Refinement for ADV_ARC.1.5C

  The interface between the TOE and the security module is according to the statements in the CC not a TSFI. Nevertheless, it has to be ensured by the evaluation that the TOE makes use of the services of the security module in the way specified by this PP and [BSI-TR-03109-2] whenever this is required by this PP (cmp. ▸Section 1.4.8 and ▸Section 3.5). Therefore, the developer has to describe in their documentation for ADV_ARC.1.5C in which way the TOE utilizes the services from the security module.

- Refinement for ADV_ARC.1-5

  Furthermore, the evaluator shall examine during the work for ADV_ARC.1-5 the security architecture description to determine that it presents an analysis that adequately describes that the TOE utilizes the services of the security module as described in this PP and [BSI-TR-03109-2].

- Refinement for ADV_IMP.1.1E

  The sample selected by the evaluator shall include those parts that make up the interface to the security module. The evaluator shall examine the relevant parts of the implementation representation to verify the developer statements from ADV_ARC.1.5C.

- Refinement for ALC_DEL.1 for the following assurance elements

ALC_DEL.1.1D: The developer shall document and provide procedures for delivery of the TOE or parts of it to the ~~consumer~~ **MPO**.

ALC_DEL.1.1C: The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the ~~consumer~~ **MPO**.

Application Note 80: In terms of the refinement for ALC_DEL.1, "MPO" as the recipient of the TOE delivery is to be understood to also mean SRV or any other agent who act as a contractor on behalf of the MPO.

6.11 Security functional requirements rationale

6.11.1 Security functional requirements rationale

6.11.1.1 Fulfilment of the security objectives

This chapter proves that the set of security requirements (TOE) is suited to fulfill the security objectives described in Chapter 4 and that each SFR can be traced back to the security objectives. At least one security objective exists for each security requirement.

	O.Firewall	O.SeparateIF	O.ConcealWAN	O.Meter	O.Crypt	O.Time	O.Protect	O.Management	O.Log	O.Access	O.KeyGenService
FAU_ARP.1/SYS									X		
FAU_GEN.1/SYS									X		
FAU_SAA.1/SYS									X		
FAU_SAR.1/SYS									X		
FAU_STG.5/SYS									X		
FAU_GEN.1/CON									X		
FAU_SAR.1/CON									X		
FAU_STG.5/CON									X		
FAU_GEN.1/CAL									X		
FAU_SAR.1/CAL									X		
FAU_STG.5/CAL									X		
FAU_GEN.2									X		
FAU_STG.3									X		
FCS_CKM.1/SERVICE					X						X
FCS_CKM.5/TLS					X						
FCS_CKM.5/CMAC					X						X
FCS_CKM.5/X963					X						
FCS_COP.1/AES					X						
FCS_COP.1/HMAC					X						
FCS_COP.1/MTRCMAC					X						
FCS_COP.1/CMSCMAC					X						
FCS_COP.1/AESWRAP					X						
FCS_COP.1/HASH					X						

	O.Firewall	O.SeparateIF	O.ConcealWAN	O.Meter	O.Crypt	O.Time	O.Protect	O.Management	O.Log	O.Access	O.KeyGenService
▸FCS_COP.1/MEM					X		X				
▸FCS_CKM.6					X						X
▸FDP_ACC.2								X	X	X	
▸FDP_ACF.1								X	X	X	
▸FDP_IFC.2	X	X		X							
▸FDP_IFF.1	X	X		X							
▸FDP_RIP.2							X				
▸FDP_SDI.2							X				
▸FIA_AFL.1										X	
▸FIA_ATD.1										X	
▸FIA_UAU.1										X	
▸FIA_UAU.5										X	
▸FIA_UID.1										X	
▸FIA_USB.1										X	
▸FMT_MOF.1								X			X
▸FMT_MTD.1								X			
▸FMT_SMF.1								X			
▸FMT_SMR.1								X			
▸FPR_CON.1			X								
▸FPR_PSE.1				X							
▸FPT_FLS.1							X				
▸FPT_PHP.1							X				
▸FPT_RPL.1					X						
▸FPT_STM.1						X			X		
▸FPT_STM.2						X			X		
▸FPT_TST.1							X				
▸FTP_PRO.1/TLS12	X			X	X				X	X	
▸FTP_PRO.2/TLS12	X			X	X				X	X	
▸FTP_PRO.3/TLS12	X			X	X				X		
▸FTP_PRO.1/TLS13	O			O	O				O	O	
▸FTP_PRO.2/TLS13	O			O	O				O	O	
▸FTP_PRO.3/TLS13	O			O	O				O		
▸FTP_PRO.1/SYM	X			X	X						
▸FTP_PRO.2/SYM	X			X	X						
▸FTP_PRO.3/SYM	X			X	X						
▸FTP_PRO.1/CMS				X							
▸FTP_PRO.2/CMS				X							

	O.Firewall	O.SeparateIF	O.ConcealWAN	O.Meter	O.Crypt	O.Time	O.Protect	O.Management	O.Log	O.Access	O.KeyGenService
▸FTP_PRO.3/CMS				X							

Table 6.12 Fulfillment of security objectives

Application Note 81: Optional SFRs of this PP are included in this table. The mapping to the security objectives is indicated by "O" for optional. If the SFRs are included in the ST, the mapping to the security objectives shall be replaced by "X". In addition, the SFRs have to be included in the rationale of the respective paragraphs below. If the SFRs are not included in the ST, the SFRs and the respective rows shall be removed from the table.

The following paragraphs contain more details on this mapping.

6.11.1.1.1 O.Firewall

O.Firewall is met by a combination of the following SFRs:

- **FDP_IFC.2** defines that the TOE shall implement an information flow policy for its firewall functionality.
- **FDP_IFF.1** defines the concrete rules for the firewall information flow policy.
- **FTP_PRO.*/TLS12** define the trusted channel to parties in the WAN, LMN and HAN.
- **FTP_PRO.*/SYM** define the trusted channel to meters that communicate unidirectionally.

6.11.1.1.2 O.SeparateIF

O.SeparateIF is met by a combination of the following SFRs:

- ▸Application Note 43 defines that **FDP_IFC.2** and **FDP_IFF.1** require the TOE to implement physically separate ports for WAN, HAN and LMN.

6.11.1.1.3 O.ConcealWAN

O.ConcealWAN is completely met by **FPR_CON.1** as directly follows.

6.11.1.1.4 O.Meter

O.Meter is met by a combination of the following SFRs:

- **FDP_IFC.2** and **FDP_IFF.1** define an information flow policy to introduce how the TOE shall handle meter data.
- **FTP_PRO.*/TLS12** defines the requirements for the trusted channel that shall be implemented by the TOE in order to protect information submitted via the TOE and external entities in the WAN or the TOE and a distributed meter.
- **FTP_PRO.*/SYM** defines the requirements for the trusted channel that shall be implemented by the TOE in order to protect information received by the TOE from a meter.
- **FTP_PRO.*/CMS** defines the requirements for encryption of data if they are sent to the final recipient via a third party.
- **FPR_PSE.1** defines requirements around the pseudonymization of meter identities for status data.

6.11.1.1.5 O.Crypt

O.Crypt is met by a combination of the following SFRs:

- **FTP_PRO.*/TLS12** and **FTP_PRO.*/SYM** ensure the usage of authenticated, integrity protected and encrypted communication channels with external entities where necessary.

- **FPT_RPL.1** ensures that a replay attack is detected for wake-up calls and for messages of unidirectionally communicating meters. **FTP_PRO.3/TLS12** ensures that a replay attack is detected for communication using TLS v1.2.
- The following SFRs detail the cryptographic methods required for the usage of the communication channels as in FTP_PRO.*/*:
  - **FCS_CKM.5/TLS** defines the requirements on key derivation for the TLS protocol.
  - **FCS_CKM.5/CMAC** defines the requirements on key derivation for unidirectional communication with meters.
  - **FCS_CKM.5/X963** defines the requirements on key derivation for key encryption keys for CMS.
  - **FCS_COP.1/AES** defines the requirements on cryptographic operation using AES for TLS, for unidirectional communication with meters and for content data encryption.
  - **FCS_COP.1/HMAC** defines the requirements on cryptographic operation using HMAC for TLS.
  - **FCS_COP.1/MTRCMAC** defines the requirements on cryptographic operation using AES-CMAC for unidirectional communication with meters.
  - **FCS_COP.1/CMSCMAC** defines the requirements on cryptographic operation using AES-CMAC for content data integrity protection and authentication.
  - **FCS_COP.1/AESWRAP** defines the requirements on cryptographic operation of key encryption for CMS.
  - **FCS_COP.1/HASH** defines the requirements on cryptographic operation using hashing for TLS, unidirectional communication with meters, content data encryption and protection.
- **FCS_CKM.1/SERVICE** defines the requirements on key generation for key distribution to HAN and LMN.
- **FCS_COP.1/MEM** defines the requirements concerning the encryption of TSF data.
- **FCS_CKM.6** defines the requirements concerning the secure deletion of ephemeral cryptographic keys and other keys generated by the TOE but no longer needed.

6.11.1.1.6 O.Time

O.Time is met by a combination of the following SFRs:

-
- **FPT_STM.1** defines that the TOE shall be able to provide reliable time stamps.
- **FPT_STM.2** defines that the GWA shall be able to adjust the time source for the SMGW time.

6.11.1.1.7 O.Protect

O.Protect is met by a combination of the following SFRs:

- **FCS_COP.1/MEM** defines that the TOE shall encrypt its TSF and user data as long as it is not in use.
- **FDP_RIP.2** defines that the TOE shall make information unavailable as soon as it is no longer needed.
- **FDP_SDI.2** defines requirements around the integrity protection for stored user data.
- **FPT_FLS.1** defines requirements that the TOE remains in a secure state for specific error cases including but not limited to integrity errors detected by **FDP_SDI.2** or **FPT_TST.1**.
- **FPT_TST.1** defines requirements for self-test functionality of the TOE.
- **FPT_PHP.1** defines the requirements for the physical protection that the TOE has to provide.

6.11.1.1.8 O.Management

O.Management is met by a combination of the following SFRs:

- **FDP_ACC.2** and **FDP_ACF.1** define the access policy also concerning the management of security functions.
- **FMT_MOF.1** defines requirements for the limitations for management of security functions.

- **FMT_MTD.1** defines requirements for the management of TSF data.
- **FMT_SMF.1** defines the management functionalities that the TOE must offer.
- **FMT_SMR.1** defines the role concept for the TOE.

6.11.1.1.9 O.Log

O.Log defines that the TOE shall implement three different audit processes that are covered by the security functional requirements as follows:

System log

The implementation of the system log itself is covered by the use of **FAU_GEN.1/SYS**. **FAU_ARP.1/SYS** and **FAU_SAA.1/SYS** allow to define a set of criteria for automated analysis of the audit and a corresponding response. **FAU_SAR.1/SYS** defines the requirements concerning the audit review functions and further the restriction of access to the system log only for authorized GWAs via the WAN interface and for authorized SRVs via the HAN-CON or HAN-CLS interface. Finally, **FAU_STG.5/SYS** defines the requirements on what should happen if the audit log is full. **FTP_PRO.*/TLS12** defines the requirements on the protection of the communication of the GWA and the SRV with the TOE.

Consumer log

The implementation of the consumer log itself is covered by the use of **FAU_GEN.1/CON**. **FAU_STG.5/CON** defines the requirements on what should happen if the audit log is full. **FAU_SAR.1/CON** defines the requirements concerning the audit review functions for the consumer log as well as the restriction of access to the consumer log only for the respective authorized consumer via the HAN-CON and HAN-CLS interface. **FTP_PRO.*/TLS12** defines the requirements on the protection of the communication of the consumer with the TOE.

Calibration log

The implementation of the calibration log itself is covered by the use of **FAU_GEN.1/CAL. FAU_STG.5/CAL** defines the requirements on what should happen if the audit log is full. **FAU_SAR.1/CAL** defines the requirements concerning the audit review functions for the calibration log and further the restriction of access to the calibration log only for authorized GWAs via the WAN interface. **FMT_MTD.1** defines that the deletion of the calibration log is limited to the authorized GWA and authorized SRV. **FTP_PRO.*/TLS12** defines the requirements on the protection of the communication of the GWA and the SRV with the TOE.

FAU_GEN.2, FAU_STG.3,, **FDP_ACC.2**, **FDP_ACF.1**, **FPT_STM.1** and **FPT_STM.2** apply to all three audit processes.

6.11.1.1.10 O.Access

O.Access is met by a combination of the following SFRs:

- **FDP_ACC.2** and **FDP_ACF.1** define the access control policy and the access rights to assets and TSF. **FMT_MOF.1** supports these SFRs by defining the access to management functionality.
- **FIA_UAU.1** ensures that entities have to be authenticated before any TSF-mediated action on behalf of these entities with the exception of access to the SMGW time.
- **FIA_UAU.5** defines the means of authentication available for external entites at the TSFI.
- **FIA_UID.1** ensures that entities have to be identified before any TSF-mediated action on behalf of these entities with the exception of access to the SMGW time.
- **FIA_AFL.1** defines the requirements if the authentication of users fails multiple times.
- **FIA_ATD.1** defines the attributes for users.
- **FIA_USB.1** defines that the TOE must be able to associate users with subjects acting on behalf of them.
- **FTP_PRO.1/TLS12** ensures that external entities are re-authenticated after the session key has been used for a certain amount of time.

6.11.1.1.11 O.KeyGenService

O.KeyGenService is met by a combination of the following SFRs:

- **FMT_MOF.1** allows CLS in the HAN and meters in the LMN to request the generation of keys and certificates.
- **FCS_CKM.1/SERVICE** defines the requirements on key generation for the keys and certificates to be distributed to entities in the HAN and LMN.
- **FCS_CKM.5/CMAC** defines the requirements on key generation for the pre-shared key for the unidirectional communication with meters based on symmetric encryption in the LMN.
- **FCS_CKM.6** defines the requirements for the secure deletion of generated cryptographic keys that are no longer needed.

6.11.1.2 Fulfilment of the dependencies

The following table summarizes all TOE functional requirements dependencies of this PP and demonstrates that they are fulfilled.

SFR	Dependencies	Fulfilled by
▸FAU_ARP.1/SYS	FAU_SAA.1	▸FAU_SAA.1/SYS
▸FAU_GEN.1/SYS	FPT_STM.1	▸FPT_STM.1
▸FAU_SAA.1/SYS	FAU_GEN.1	▸FAU_GEN.1/SYS
▸FAU_SAR.1/SYS	FAU_GEN.1	▸FAU_GEN.1/SYS
▸FAU_STG.5/SYS	FAU_STG.2	▸FAU_STG.3
	FAU_GEN.1	▸FAU_GEN.1/SYS
▸FAU_GEN.1/CAL	FPT_STM.1	▸FPT_STM.1
▸FAU_SAR.1/CAL	FAU_GEN.1	▸FAU_GEN.1/CAL
▸FAU_STG.5/CAL	FAU_STG.2	▸FAU_STG.3
	FAU_GEN.1	▸FAU_GEN.1/CAL
▸FAU_GEN.1/CON	FPT_STM.1	▸FPT_STM.1
▸FAU_SAR.1/CON	FAU_GEN.1	▸FAU_GEN.1/CON
▸FAU_STG.5/CON	FAU_STG.2	▸FAU_STG.3
	FAU_GEN.1	▸FAU_GEN.1/CON
▸FAU_GEN.2	FAU_GEN.1	▸FAU_GEN.1/SYS ▸FAU_GEN.1/CON ▸FAU_GEN.1/CAL
	FIA_UID.1	▸FIA_UID.1
▸FAU_STG.3	FAU_GEN.1	▸FAU_GEN.1/SYS ▸FAU_GEN.1/CON ▸FAU_GEN.1/CAL
▸FCS_CKM.1/SERVICE	[FCS_CKM.2 *or* FCS_CKM.5 *or* FCS_COP.1]	The key generated as modelled in FCS_CKM.1/SERVICE are distributed via the trusted path between the TOE and the respective external entities that is also used for other communication (which is modelled via FTP_PRO/TLS). Hence, this dependency is omitted.
	[FCS_RBG.1 *or* FCS_RNG.1]	The randomness required for these SFRs is provided by the functionality of the security module. As such, the dependency to FCS_RNG.1 is implicitly fulfilled by the operational environment.

SFR	Dependencies	Fulfilled by
	FCS_CKM.6	▸FCS_CKM.6
▸FCS_CKM.5/CMAC	[FCS_CKM.2 *or* FCS_COP.1]	▸FCS_COP.1/AES ▸FCS_COP.1/MTRCMAC
	FCS_CKM.6	▸FCS_CKM.6
▸FCS_CKM.5/TLS	[FCS_CKM.2 *or* FCS_COP.1]	▸FCS_COP.1/AES
	FCS_CKM.6	▸FCS_CKM.6
▸FCS_CKM.5/X963	[FCS_CKM.2 *or* FCS_COP.1]	▸FCS_COP.1/AESWRAP
	FCS_CKM.6	▸FCS_CKM.6
▸FCS_CKM.6	[FDP_ITC.1 *or* FDP_ITC.2 *or* FCS_CKM.1 *or* FCS_CKM.5]	▸FCS_CKM.1/SERVICE ▸FCS_CKM.5/TLS ▸FCS_CKM.5/CMAC ▸FCS_CKM.5/X963
▸FCS_COP.1/AES	[FDP_ITC.1 *or* FDP_ITC.2 *or* FCS_CKM.1 *or* FCS_CKM.5]	▸FCS_CKM.5/TLS
	FCS_CKM.6	▸FCS_CKM.6
▸FCS_COP.1/AESWRAP	[FDP_ITC.1 *or* FDP_ITC.2 *or* FCS_CKM.1 *or* FCS_CKM.5]	▸FCS_CKM.5/X963
	FCS_CKM.6	▸FCS_CKM.6
▸FCS_COP.1/CMSCMAC	[FDP_ITC.1 *or* FDP_ITC.2 *or* FCS_CKM.1 *or* FCS_CKM.5]	This has to be clarified by the ST author, see ▸Section 6.3.9.
	FCS_CKM.6	▸FCS_CKM.6
▸FCS_COP.1/HASH	[FDP_ITC.1 *or* FDP_ITC.2 *or* FCS_CKM.1 *or* FCS_CKM.5]	The hash algorithm does not need any key material. As such the dependency to an import or generation of key material is omitted for this SFR.
	FCS_CKM.6	▸FCS_CKM.6
▸FCS_COP.1/HMAC	[FDP_ITC.1 *or* FDP_ITC.2 *or* FCS_CKM.1 *or* FCS_CKM.5]	▸FCS_CKM.5/TLS
	FCS_CKM.6	▸FCS_CKM.6

SFR	Dependencies	Fulfilled by
▸FCS_COP.1/MEM	[FDP_ITC.1 *or* FDP_ITC.2 *or* FCS_CKM.1 *or* FCS_CKM.5]	This has to be clarified by the ST author, see ▸Section 6.3.12.
	FCS_CKM.6	▸FCS_CKM.6
▸FCS_COP.1/MTRCMAC	[FDP_ITC.1 *or* FDP_ITC.2 *or* FCS_CKM.1 *or* FCS_CKM.5]	▸FCS_CKM.5/CMAC
	FCS_CKM.6	▸FCS_CKM.6
▸FDP_ACC.2	FDP_ACF.1	▸FDP_ACF.1
▸FDP_ACF.1	FDP_ACC.1	▸FDP_ACC.2
	FMT_MSA.3	The security attributes for the SMGW access SFP are fixed and cannot be changed, hence, no default values (to be configured by the GWA) are necessary. Thus, this SFR is omitted.
▸FDP_IFC.2	FDP_IFF.1	▸FDP_IFF.1
▸FDP_IFF.1	FDP_IFC.1	▸FDP_IFC.2
	FMT_MSA.3	The security attributes for the SMGW access SFP are fixed and cannot be changed, hence, no default values (to be configured by the GWA) are necessary. Thus, this SFR is omitted.
▸FDP_RIP.2	-	-
▸FDP_SDI.2	-	-
▸FIA_AFL.1	FIA_UAU.1	▸FIA_UAU.1
▸FIA_ATD.1	-	-
▸FIA_UAU.1	FIA_UID.1	▸FIA_UID.1
▸FIA_UAU.5	-	-
▸FIA_UID.1	-	-
▸FIA_USB.1	FIA_ATD.1	▸FIA_ATD.1
▸FMT_MOF.1	FMT_SMR.1	▸FMT_SMR.1
	FMT_SMF.1	▸FMT_SMF.1
▸FMT_MTD.1	FMT_SMR.1	▸FMT_SMR.1
	FMT_SMF.1	▸FMT_SMF.1
▸FMT_SMF.1	-	-
▸FMT_SMR.1	FIA_UID.1	▸FIA_UID.1
▸FPR_CON.1	-	-
▸FPR_PSE.1	-	-
▸FPT_FLS.1	-	-
▸FPT_PHP.1	-	-
▸FPT_RPL.1	-	-
▸FPT_STM.1	-	-
▸FPT_STM.2	FPT_STM.1	▸FPT_STM.1
	FMT_SMR.1	▸FMT_SMR.1

SFR	Dependencies	Fulfilled by
▸FPT_TST.1	-	-
▸FTP_PRO.1/CMS	FTP_PRO.2	▸FTP_PRO.2/CMS
	FTP_PRO.3	▸FTP_PRO.3/CMS
▸FTP_PRO.2/CMS	FTP_PRO.1	▸FTP_PRO.1/CMS
	[FCS_CKM.1 *or* FCS_CKM.2]	The key encryption keys are generated and provided by the security module using ECKA-DH. As such, the dependency to FCS_CKM.1 is implicitly fulfilled by the operational environment.
	FCS_CKM.5	▸FCS_CKM.5/X963
	FCS_COP.1	▸FCS_COP.1/AESWRAP
▸FTP_PRO.3/CMS	FTP_PRO.1	▸FTP_PRO.1/CMS
	FTP_PRO.2	▸FTP_PRO.2/CMS
	FCS_COP.1	▸FCS_COP.1/AES ▸FCS_COP.1/CMSCMAC[24]
▸FTP_PRO.1/SYM	FTP_PRO.2	▸FTP_PRO.2/SYM
	FTP_PRO.3	▸FTP_PRO.3/SYM
▸FTP_PRO.2/SYM	FTP_PRO.1	▸FTP_PRO.1/SYM
	[FCS_CKM.1 *or* FCS_CKM.2]	The initial shared key with a meter is generated by the meter or their developer and brought into the TOE by the GWA using the management functionality of ▸FMT_SMF.1. As such, the dependency to FCS_CKM.2 is implicitly fulfilled.
	FCS_CKM.5	▸FCS_CKM.5/CMAC
	FCS_COP.1	▸FCS_COP.1/MTRCMAC
▸FTP_PRO.3/SYM	FTP_PRO.1	▸FTP_PRO.1/SYM
	FTP_PRO.2	▸FTP_PRO.2/SYM
	FCS_COP.1	▸FCS_COP.1/AES ▸FCS_COP.1/MTRCMAC
▸FTP_PRO.1/TLS12	FTP_PRO.2	▸FTP_PRO.2/TLS12
	FTP_PRO.3	▸FTP_PRO.3/TLS12
▸FTP_PRO.2/TLS12	FTP_PRO.1	▸FTP_PRO.1/TLS12
	[FCS_CKM.1 *or* FCS_CKM.2]	The keys are generated and provided by the security module. As such, the dependency to FCS_CKM.1 is implicitly fulfilled by the operational environment.
	FCS_CKM.5	▸FCS_CKM.5/TLS
	FCS_COP.1	The establishment of a shared secret which is modelled in ▸FTP_PRO.2/TLS12 uses ECKA-DH provided by the security module. As such, the dependency to FCS_COP.1 is implicitly fulfilled by the operational environment.
▸FTP_PRO.3/TLS12	FTP_PRO.1	▸FTP_PRO.1/TLS12
	FTP_PRO.2	▸FTP_PRO.2/TLS12
	FCS_COP.1	▸FCS_COP.1/AES ▸FCS_COP.1/HMAC

[24] This dependency is partially fulfilled by the operational environment as the security module provides ECDSA.

SFR	Dependencies	Fulfilled by
▸FTP_PRO.1/TLS13	FTP_PRO.2	▸FTP_PRO.2/TLS13
	FTP_PRO.3	▸FTP_PRO.3/TLS13
▸FTP_PRO.2/TLS13	FTP_PRO.1	▸FTP_PRO.1/TLS13
	[FCS_CKM.1 *or* FCS_CKM.2]	The keys are generated and provided by the security module using ECKA-DH. As such, the dependency to FCS_CKM.1 is implicitly fulfilled by the operational environment.
	FCS_CKM.5	▸FCS_CKM.5/TLS
	FCS_COP.1	The establishment of a shared secret which is modelled in ▸FTP_PRO.2/TLS13 uses ECDHE provided by the security module. As such, the dependency to FCS_COP.1 is implicitly fulfilled by the operational environment.
▸FTP_PRO.3/TLS13	FTP_PRO.1	▸FTP_PRO.1/TLS13
	FTP_PRO.2	▸FTP_PRO.2/TLS13
	FCS_COP.1	▸FCS_COP.1/AES

Table 6.13 SFR Dependencies

Application Note 82: Optional SFRs of this PP are included in this table. If the SFRs are included in the ST, the respective entries shall be included. If the SFRs are not included in the ST, the respective entries shall be removed.

6.11.2 Security assurance requirements rationale

The decision on the assurance level has been mainly driven by the assumed attack potential. As outlined in the previous chapters of this PP it is assumed that – at least from the WAN side – a high attack potential is posed against the security functions of the TOE. This leads to the use of AVA_VAN.5 (Resistance against high attack potential).

In order to keep evaluations according to this PP commercially feasible, EAL4 has been chosen as assurance level, as this is the lowest level that provides the prerequisites for the use of AVA_VAN.5.

Eventually, the augmentation by ALC_FLR.2 has been chosen to emphasize the importance of a structured process for flaw remediation at the developer’s side, specifically for such a new technology.

6.11.2.1 Dependencies of assurance components

The dependencies of the assurance requirements taken from EAL4 are fulfilled automatically. The augmentation by AVA_VAN.5 and ALC_FLR.2 does not introduce additional assurance components that are not contained in EAL4.

7 Functional packages

7.1 Functional packages overview

This PP utilizes the concept of functional packages. For the use of this PP, it is not required to add any of the functional packages described in this chapter. However, any functional package from this PP shall never be used without the base PP.

▸Table 7.1 identifes the functional packages that can be used to achieve the description of certain use cases that have been considered during the development of this PP. If the TOE is intended to implement the functionality of a use case or intended to operate in the environment described in a use case, the mapped functional package shall be used.

Use Case	Functional package power limitation
TOE used for controlling of CLS	X

Table 7.1 Functional packages for use cases

7.2 Functional package: Power limitation

7.2.1 Package identification

Title	Power limitation functional package
Short title	PowerLimFp
Version	1.0
Date	This functional package inherits the date of the base PP. Please refer to ▸Section 1.2.
Sponsor	This functional package inherits the sponsor of the base PP. Please refer to ▸Section 1.2.
Registration	This functional package inherits the certification ID of the base PP. Please refer to ▸Section 1.2.
CC Version	CC:2022 Revision 1
Conformance claim	• The conformance of this package is Common Criteria ([CC]) Part II conformant • The conformance of this package is Common Criteria ([CC]) Part III conformant

Table 7.2 Identification of functional package power limitation

7.2.2 Package overview

This functional package shall be used if the TOE supports controlling of CLS directly in the following way: For a CLS, the GWA configures a controlling profile on the TOE. This controlling profile contains information such as

- the CLS identification,
- external entities associated with the CLS,
- information on the kind of commands sent to the CLS for controlling.

In particular, the controlling profile describes for the TOE how to process control data. Containing e.g. limits on power consumption or production, these control data are sent from the GWA to the TOE, which stores them, possibly processes them, and allows for CLS to read these control data. In addition, notifications of CLS about the reception of such control data may be received, possibly processed, and stored by the TOE. The TOE may provide signatures for these notifications, using the functionality of the security module. These notifications may be sent by the TOE to the GWA or an external market participant.

This functional package covers e.g. the use cases of

- limitation of power consumption,
- limitation of power production,

- monitoring,

but is not limited to these use cases.

The threat model in ▸Chapter 3 does not cover these data, their need for protection or threats against them. Therefore, the following section describes a security problem definition for these use cases. This security problem definition adds to the security problem definition of the base PP, and that this functional package shall only be used in combination with the base PP.

Application Note 83: Note that in case this functionality is described and detailed in [BSI-TR-03109-1], the ST author shall model the functionality in this PP consistently with the requirements therein. Further information may be provided in accompanying documents to [BSI-TR-03109-1].

The ST author shall then also add the information concerning this functionality in ▸Section 1.4.3 as well as in ▸Section 1.4.6 as a separate security feature.

7.2.3 Security problem definition

7.2.3.1 Assets

The following assets shall be added to ▸Table 3.2 if this functional package is chosen.

Asset	Description	Need for protection	User/TSF data
Controlling profile	A controlling profile is associated with a CLS and contains information and commands to control that CLS. It further contains information on external entities associated with the CLS.	• Integrity and authenticity	TSF data
Control data	Data containing information and commands to control CLS such as limits on power consumption or power production.	• Integrity and authenticity	user data
Control data receipt	Data containing information about the acknowledgement and reception of control data by a CLS. May contain information concerning the monitoring of power consumption or production.	• Integrity and authenticity	user data

Table 7.3 Assets for the functional package power limitation

7.2.3.2 Assumptions

The following assumptions shall be added to the ST if this functional package is chosen.

A.ControllingProfile The controlling profiles that are used when handling data are assumed to be trustworthy and correct.

7.2.3.3 Threats

The following threats shall be added to the ST if this functional package is chosen.

T.ModificationControlling A local attacker or remote attacker may try modify (i.e., alter, delete, insert, replay or redirect) controlling profiles, control data or control data receipts on the TOE or during the transmission between the TOE and an external entity.

Note that by adding the assets in ▸Section 7.2.3.1, all threats addressing user data and/or TSF data include the respective assets of this section as a target.

7.2.3.4 OSP

This package does not contain any additional OSP. However, the following OSP from the base PP has to be adjusted as follows.

OSP	Adjustment
OSP.Log	• System log: The system log shall log relevant events concerning the assets controlling profile, control data and control data receipt. • Consumer log: The consumer log shall contain information about data sent to or from the TOE based on controlling profiles for CLS devices associated with the consumer.

Table 7.4 Adjustments to OSPs from the base PP for the functional package power limitation

7.2.4 Security objectives

7.2.4.1 Security objectives for the TOE

This package does not contain any additional security objectives for the TOE. However, the following security objectives for the TOE from the base PP have to be adjusted as follows.

Security objective for the TOE	Adjustment
O.Management	• The authorized GWA may create, modify and delete controlling profiles on the TOE. Further, the GWA may write control data to the TOE. • The authorized CLS may write control data receipts to the TOE.
O.Log	• System log: The system log shall log relevant events concerning the assets controlling profile, control data and control data receipt. • Consumer log: The consumer log shall contain information about data sent to or from the TOE based on controlling profiles for CLS devices associated with the consumer.

Table 7.5 Adjustments to security objectives from the base PP for the functional package power limitation

7.2.4.2 Security objectives for the environment

The following security objectives for the environment shall be added to the ST if this functional package is chosen.

OE.ControllingProfile The controlling profiles that are used when handling control data shall be trustworthy and correct.

7.2.4.3 Security objectives rationale

7.2.4.3.1 Overview

	O.Crypt	O.Protect	O.Management	O.Access	O.Log	OE.TrustedAdmins	OE.PhysicalProtection	OE.ControllingProfile
T.ModificationControlling	X	X	X	X		X	X	
OSP.Log		X	X	X	X	X		
A.ControllingProfile								X

Table 7.6 Rationale for security objectives of functional package power limitation

In the following paragraphs, the mapping in the table is described in more detail.

7.2.4.3.2 General objectives

For the security problem definition of the base PP, the security objectives **O.Protect**, **O.Management** and **OE.TrustedAdmins** contribute to counter each threat and contribute to each OSP. This also holds for **T.Mo-**

dificationControlling and **OSP.Log** of this functional package, thus, these security objectives will not be addressed in detail in the following paragraphs.

7.2.4.3.3 T.ModificationControlling

The threat **T.ModificationControlling** is countered by a combination of the security objectives **O.Crypt** and **OE.ControllingProfile**.

O.Crypt defines the required cryptographic functionality for the communication to external entities.

O.Access ensures that only those external entities with access rights may read or modify the controlling profiles, control data or control data receipts.

OE.PhysicalProtection is of relevance in case of a local attacker with physical access as it ensures that access to the TOE is limited.

7.2.4.3.4 OSP.Log

The rationale for the mapping of **OSP.Log** contains no changes from the base PP.

7.2.4.3.5 A.ControllingProfile

The assumption **A.ControllingProfile** is directly and completely covered by the security objective **OE.ControllingProfile.** The assumption and the objective for the environment are drafted in a way that the correspondence is obvious.

7.2.5 Application notes

Per CC Pt1 Annex 1, audit and management requirements relating to the SFRs of the subsequent section shall be specified in this section.

7.2.5.1 Audit requirements for the system log

FAU_GEN.1/SYS: The events and information listed in ▸Table 6.3 remain unchanged. However, the events of the following SFRs are affected:

- FDP_ACF.1
- FDP_IFF.1
- FMT_MOF.1
- FMT_SMF.1

7.2.5.2 Management requirements

FMT_SMF.1: The referred ▸Table 6.7 has additional entries.

7.2.5.3 Further information

Note that via the adjustment of the SFRs in the following section, further existing – but unchanged – SFRs are affected. E.g. FDP_ACC.2.1 refers to all assets as defined in ▸Table 3.2. By adding this functional package, the referred table includes additional assets that are covered by this element. These SFRs are listed here:

- FDP_ACC.2: new assets control data and control data receipt are covered by the SFP.
- FDP_RIP.2: Further user and TSF data have to be deleted securely when no longer in use.
- FDP_SDI.2: The integrity protection covers a wider range of user data.

7.2.6 Security functional requirements

The following security functional requirements shall be *adjusted from the base PP* if this functional package is chosen.

7.2.6.1 FAU_GEN.1/CON

The following events shall be added to ▸Table 6.4:

Event	Additional information
Any change to a controlling profile associated with the consumer's CLS	• In case of a new controlling profile, the whole controlling profile • In case of a change of an existing controlling profile, the ID of the profile and the updated values of the controlling profile • In case of a deleted controlling profile, the ID of the profile
Any submission of control data to the consumer's CLS	The control data sent to the CLS
Any submission of a control data receipt from the consumer's CLS to the TOE	The control data receipt sent from the CLS

Table 7.7 Additional events for consumer log in functional package power limitation

7.2.6.2 FDP_ACF.1

The following rules shall be added to Table 6.6:

Subject	Object	operation / type of access	interface
authorized consumer	controlling profile (only the controlling profiles for CLS associated with the consumer)	read access	HAN-CON or HAN-CLS
	the control data and control data receipt		
authorized GWA	controlling profile	operation and access as described in Table 6.7[25]	WAN
	control data		
	control data receipt	read access	
authorized CLS	meter data (only the current meter data associated with the CLS according to a controlling profile)	read access	HAN-CON or HAN-CLS
	controlling profile		
	control data		
	control data receipt	operation and access as described in Table 6.7[footnote 7.1]	

Table 7.8 Additional rules for the SMGW access SFP in functional package power limitation

7.2.6.3 FDP_IFF.1

The SFR shall be adjusted as follows:

In element **FDP_IFF.1.2**, the following bullet point from the list of rules shall be adjusted:

- an information flow between the TOE and external entities shall be according to the rules set in a corresponding communication profile, processing profile, or controlling profile,

7.2.6.4 FMT_MOF.1

The following rules shall be added to Table 6.7:

[25] The reference to the table of FMT_MOF.1 assumes that the entries according to Table 7.9 will be added in the ST.

Subject	Object
Management of controlling profiles	The authorized GWA is allowed to read and write the controlling profiles.
Management of control data	The authorized GWA is allowed to read and write the control data.
Control data receipt	The authorized CLS is allowed to send, i.e., write control data receipts to the TOE.

Table 7.9 Additional restrictions on management functions in functional package power limitation

7.2.6.5 Security functional requirments rationale

As there are no new but only adjusted security objectives for the TOE (**O.Management** and **O.Log**), the following rationale focusses on these adjusted security objectives and only on those SFRs that map to the adjusted part of the security objectives. Therefore, the mapping table is omitted. The rationale for the mapping of these SFRs shall be added to the rationale of the base PP.

	O.Management	O.Access	O.Log
▸FAU_GEN.1/CON			X
▸FDP_ACC.2 x	X	X	X
▸FDP_ACF.1 x	X	X	X
▸FDP_IFC.2			
▸FDP_IFF.1			
▸FMT_MOF.1	X		

Table 7.10 Fulfillment of security objectives for functional package power limitation

7.2.6.5.1 O.Management

The additional content in O.Management is met by the following SFRs:

- **FDP_ACC.2** and **FDP_ACF.1** define the access policy concerning the read and write access of controlling profiles, control data and control data receipts. **FDP_ACF.1** is adjusted accordingly.
- **FMT_MOF.1** defines requirements for the limitations for management of controlling profiles, control data and control data receipts. It is adjusted accordingly.

7.2.6.5.2 O.Access

O.Access remains unchanged, however, the new assets implicitly adjust O.Access. The security objective for access to these additional assets is met by the following SFRs:

- **FDP_ACC.2** and **FDP_ACF.1** define the access policy concerning the read and write access of controlling profiles, control data and control data receipts. **FDP_ACF.1** is adjusted accordingly.
- **FMT_MOF.1** supports these SFRs by defining the access to additional management functionality concerning controlling profiles, control data and control data receipts. It is adjusted accordingly.

7.2.6.5.3 O.Log

The additional content in O.Log is met by the following SFRs:

System log

The additional or adjusted events of the affected SFRs are covered by the use of **FAU_GEN.1/SYS**.

Consumer log

The additional information that has to be logged is covered by the use of **FAU_GEN.1/CON**.

Appendix A Mapping from English to German terms

English term	German term
billing-relevant	abrechnungsrelevant
devices for value-added services	Geräte für Mehrwertdienste
CLS, controllable local system	dezentral steuerbare Verbraucher- oder Erzeugersysteme oder Geräte für Mehrwertdienste
communication profile	Kommunikationsprofil
consumer	Anschlussnutzer Letztverbraucher (im verbrauchenden Sinne) u.U. auch Einspeiser
consumption data	Verbrauchsdaten
controlling profile	Steuerungsprofil
grid	Netz (für Strom/Gas/Wasser)
grid connection point	Netzanschlusspunkt
grid status data	Zustandsdaten des Versorgungsnetzes
industrial meter	Moderne Messeinrichtung, deren Messwerte keine personenbeziehbaren Informationen enthalten.
LMN, local metrological network	Lokales Messeinrichtungsnetz
meter	Messeinrichtung (Teil eines Messsystems)
MPO, metering point operator	Messstellenbetreiber
processing profile	Auswertungsprofil
security module	Sicherheitsmodul (z.B. eine Smart Card)
service provider	Diensteanbieter
SMGW, smart meter gateway	Kommunikationseinheit eines intelligenten Messsystems
smart metering system	intelligentes Messsystem
residential meter	Moderne Messeinrichtung, deren Messwerte personenbeziehbaren Informationen enthalten können.
TOE, target of evaluation	EVG (Evaluierungsgegenstand)
WAN, wide area network	Weitverkehrsnetz (für Kommunikation)

Table A.1 Mapping from English to German terms

Glossary

authenticity

The property that an entity is what it claims to be (according to [SD_6]).

CLS

Controllable local system.

External entity that is a system containing IT-components in the HAN that may use the SMGW for dedicated communication purposes.

CLS may range from local power generation plants, controllable loads such as heat pumps, EV chargers or battery storage to applications in home automation. In addition, devices for value-added services, such as heat cost allocators, as well as industrial meters in the HAN of the SMGW are summarized under the term CLS.[26]

See ▸Section 3.1.

CLS config

See ▸Section 3.2.

CMS

cryptographic message syntax

commodity

Electricity, gas, water or heat. Distributed from its generator to the consumer through a grid (network).[27]

communication adapter

Component within the physical device (acc. to ▸Figure 1.3) used to provide access to a connected network. One communication adapter might provide access to different networks. [28]

confidentiality

The property that information is not made available or disclosed to unauthorised individuals, entities, or processes (according to [SD_6]).

connection

Within this document, an existing connection-oriented communication channel for realizing an information flow between one instance/role defined in ▸Section 3.1 and the SMGW.

connection establishment

The connection establishment is necessary to realize a connection between one instance or role defined in ▸Section 3.1 and the SMGW within the scenario depicted in ▸Figure 1.1, on layer 4 and below (e.g. TCP handshakes etc.).

consumer

End user of electricity, gas, water or heat. The consumer can also generate energy using a distributed energy resource. That is, the consumer also includes producers or so-called prosumers.

In terms of this document, the consumer is an external entity that interacts with the SMGW via HAN-CON or HAN-CLS. See ▸Section 3.1.

control data

Data containing information and commands to control CLS, e.g., limits on power consumption or power production. See ▸Section 7.2.3.1.

EAL

Evaluation assurance level

external entity

Human or IT entity possibly interacting with the TOE from outside of the TOE boundary. See ▸Section 3.1.

[26] The term CLS was coined in the first version of the PP, where controllable local systems (hence CLS) were considered to be connected to the SMGW. The range of use cases has since been widened; the term CLS will be used as a hypernym including the new use cases for reasons of consistency.

[27] Please note that this list does not claim to be complete.

[28] Note that the communication adapter in the context of this PP does not coincide with the communication adapter defined in [BSI-TR-03109-5].

external market participant
External entity connected to the SMGW via WAN which offers backend systems for the smart metering system in order to receive consumption or grid status data or controls CLS devices connected to the SMGW. The connection between external market participant and SMGW is configured by the GWA with corresponding profiles in the SMGW. See ▸Section 3.1.

firmware update
See ▸Section 3.2.

grid connection point
The point in a commodity network where customers are connected to the grid of that commodity.

GWA
Gateway administrator. External entity that configures, monitors, and controls the SMGW via the WAN interface. See ▸Section 3.1.

HAN
Home area network. In-house data communication network, which interconnects IT equipment with the SMGW and can e.g. be used for energy management purposes.

industrial meter
Meter, whose data are associated with a legal entity. Industrial meters are located in the LMN or in the HAN. If industrial meters are located in the LMN, their data are considered meter data. The meter data generated by the industrial meter are not considered personally identifiable information. See also residential meter.

integrity
The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner (according to [SD_6]).

local attacker
See ▸Section 3.4.

LMN
Local metrological network. In-house data communication network which connects meters with the SMGW.

meter
The term meter refers to a unit for measuring the consumption or production of a certain commodity with additional functionality. It collects consumption or production data and transmits this data to the SMGW. As not all aspects of a smart meter according to [TR50572] are implemented, in the descriptions within this document the term meter is used.

The meter has to be able to encrypt and sign the data it sends.

Please note that the term meter refers to metering devices for all kinds of commodities. It is a hypernym for residential and industrial meters in the LMN. It does not include industrial meters in the HAN.

See ▸Section 3.1.

meter config
See ▸Section 3.2.

meter data
Meter readings that allow calculation of the quantity of a commodity, for example electricity, gas, water or heat consumed or produced over a period. This includes already time-stamped meter values as well as load time series of meters. Other readings and data may also be included[29] (such as quality data, events and alarms).

Data sent to the SMGW by industrial meters in the HAN are not considered meter data.

See ▸Section 3.2.

MPO
Metering point operator. External entity which is responsible for parts of the delivery, for the installation and operation of SMGWs and meters as well as for the secure connection with CLS devices.

[29] Please note that these readings and data may require an explicit endorsement of the consumer.

PII Personally identifiable information. Refers to information that can be used to uniquely identify, contact, or locate a natural person or that can be used with other sources to uniquely identify a single individual. In the context of this PP, PII refer to natural persons that interact with the TOE in the role of consumer (CON). Note that e.g. CLS data of CLS associated with the user id of a consumer may be PII of that consumer.

PP Protection profile. Implementation-independent statement of security needs for a *TOE* type.

premises of the consumer The building where the consumer consumes or produces commodities or another building in the immediate vicinity on the same property.

PSK Pre-shared key. A key used for symmetric encryption between two parties that has been shared between these parties prior to usage.

remote attacker See ▸Section 3.4.

residential meter Meter, whose meter data are usually associated with a natural person. Residential meters are only located in the LMN. The meter data generated by the residential meter may contain personally identifiable information. See also industrial meter.

secure state State in which all data related to the TOE security functionality are correct, and security functionality remains in place.

security module A security device utilized by the SMGW for cryptographic support – typically realized in form of an integrated chip. The complete description of the security module can be found in [SecMod-PP].

smart grid A *commodity* network that intelligently integrates the behaviour and actions of all entities connected to it – suppliers of natural resources and energy, its consumers and those that are both – in order to efficiently ensure a more sustainable, economic and secure supply of that commodity (definition adopted from [TR50572]).

smart metering system A meter connected to a communication network via an SMGW.

SMGW Smart meter gateway. Device or unit responsible for collecting meter data, processing meter data, providing communication services for devices in the LMN, protecting devices in the HAN and LMN against attacks from the WAN, and providing cryptographic primitives (in cooperation with a security module).

SMGW time See ▸Section 3.2.

SRV Service technician. External entity that is responsible for the installation of the SMGW and for diagnostic purposes via the HAN interface. See ▸Section 3.1.

ST Security target. Implementation-dependent statement of security requirements for a *TOE*.

TLS Transport layer security protocol according to [RFC5246] or [RFC8446].

TOE Target of evaluation. Set of software, firmware and/or hardware possibly accompanied by guidance.

user Human, technical system or one of its components interacting with TOE from outside of the TOE boundary.

WAN

Wide area network. Extended data communication network connecting a large number of communication devices over a large geographical area.

In this document, the WAN refers to the network secured by the smart metering PKI, see [BSI-TR-03109-4].

WAN communication parameters

Non-TSF parameters used to configure the network access of the WAN communication adapter and the access to the wake-up-service of the TOE in the WAN.

References

[AIS32] *Anwendungshinweise und Interpretationen zum Schema (AIS) - AIS 32. CC-Interpretationen im deutschen Zertifizierungsschema.* Zertifizierungsstelle des BSI. 2011.

[BSI-TR-02102-1] *BSI TR-02102-1: Kryptographische Verfahren und Schlüssellängen.* current version. Bundesamt für Sicherheit in der Informationstechnik.

[BSI-TR-03109-1] Bundesamt für Sicherheit in der Informationstechnik. *Technische Richtlinie TR-03109-1: Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems.* current version.

[BSI-TR-03109-1-VIII] Bundesamt für Sicherheit in der Informationstechnik. *Technische Richtlinie BSI-TR-03109-1, Anlage VIII: Lebenszyklus.* current version.

[BSI-TR-03109-2] *Technische Richtlinie BSI-TR-03109-2: Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls.* current version. Bundesamt für Sicherheit in der Informationstechnik.

[BSI-TR-03109-3] *Technische Richtlinie BSI-TR-03109-3: Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen.* current version. Bundesamt für Sicherheit in der Informationstechnik.

[BSI-TR-03109-4] *Technische Richtlinie BSI-TR-03109-4: Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways.* current version. Bundesamt für Sicherheit in der Informationstechnik.

[BSI-TR-03109-5] Bundesamt für Sicherheit in der Informationstechnik. *Technische Richtlinie TR-03109-5: Kommunikationsadapter.* current version.

[BSI-TR-03111] *Technische Richtlinie BSI-TR-03111 Elliptic Curve Cryptography.* current version. Bundesamt für Sicherheit in der Informationstechnik.

[CC:2022] *Common Criteria for Information Technology Security Evaluation, CC:2022, Revision 1.* CCDB/ISO.

[EN13757-4] *DIN EN 13757-4:2019-09, Kommunikationssysteme für Zähler – Teil 4: Drahtlose M-Bus-Kommunikation. Englische Fassung EN 13757-4:2019. DIN/CEN/TC 294.* 2019. DIN/CEN TC294.

[EN13757-7] *DIN EN 13757-7 - Kommunikationssysteme für Zähler - Teil 7: Transport- und Sicherheitsdienste.* 2018. DIN/CEN TC294.

[MSB-LK] *Anforderungskatalog zur MSB-Lieferkette.* current version. Bundesamt für Sicherheit in der Informationstechnik.

[MsbG] *Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz - MsbG).* Bundesministerium für Wirtschaft und Klimaschutz.

[NIST-FIPS-180-4] *Secure Hash Standard (SHS).* NIST. 2015.

[NIST-FIPS-197] *Advanced Encryption Standard (AES).* NIST. 2001.

[NIST-SP800-38A] *Recommendation for Block Cipher Modes of Operation: Methods and Techniques.* NIST and M. Dworkin. 2001.

[NIST-SP800-38C] *The CCM Mode for Authentication and Confidentiality.* NIST and M. Dworkin. 2007.

[NIST-SP800-38D] *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.* NIST and M. Dworkin. 2007.

[Package_MultipleGcp] *Annex to Protection Profile for a Smart Meter Gateway (SMGW-PP) - Functional Package Multiple Grid Connection Points.* Bundesamt für Sicherheit in der Informationstechnik.

[RFC2104] IETF, H. Krawczyk, M. Bellare and R. Canetti. *HMAC: Keyed-Hashing for Message Authentication.* 1997.

[RFC3394] *Advanced Encryption Standard (AES) Key Wrap Algorithm.* IETF, J. Schaad and R. Housley. 2002.

[RFC3565] *Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS).* IETF and J. Schaad. 2003.

[RFC4493] *The AES-CMAC Algorithm.* IETF, TH Song, R. Poovendran, J. Lee and T. Iwata. 2006.

[RFC5083] *Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type.* IETF and R. Housley. 2007.

[RFC5084] *Using AES-CCM and AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS).* IETF and R. Housley. 2007.

[RFC5246] *The Transport Layer Security (TLS) Protocol Version 1.2.* IETF, T. Dierks and E. Rescorla. 2008.

[RFC5289] *TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM).* IETF and E. Rescorla. 2008.

[RFC5652] *Cryptographic Message Syntax (CMS).* IETF and R. Housley. 2009.

[RFC7027] *Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS).* IETF, J. Merkle and M. Lochter. 2013.

[RFC7366] *Encrypt-then-MAC for Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS).* IETF and P. Gutmann. 2014.

[RFC8422] *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier.* IETF, Y. Nir, S. Josefsson and M. Pegourie-Gonnard. 2018.

[RFC8446] *The Transport Layer Security (TLS) Protocol Version 1.3.* IETF. August 2018.

[RFC8734] *Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS) Version 1.3.* IETF. February 2020.

[SD_6] *ISO/IEC JTC 1/SC 27 N7446. Standing Document 6 (SD6): Glossary of IT Security Terminology.* ISO/IEC JTC 1/SC. 2009.

[SecMod-PP] *Common Criteria Protection Profile for a Security Module for Smart Metering Systems (BSI-CC-PP-0077).* current version.

[TR50572] *Functional reference architecture for communications in smart metering systems.* CEC/CLC/ETSI. 2011.

Appendix B Changelog

This table lists the major changes from version 1.3 to version 2.0. Note that this changelog will be removed before publication.

Reference in v2.0	Changes in comparison to v1.3
document wide	The PP claims conformance to [CC:2022]. Document wide adjustments have been made.
▸Section 1.1	The introduction has been reworked and updated.
▸Section 1.3, ▸Glossary	The table with specific terms in Section 1.3 has been removed and merged into the glossary table ▸Glossary for a reduction of redundancies. The glossary table has been reworked along the other changes.
document wide	It has been clarified which parts of the SMGW constitute the TOE. The terms "SMGW"/"gateway" are no longer used as a synonym for "TOE".
document wide, ▸Glossary	The term "CLS" is now also used for devices for value-added services such as heat cost allocators. Further, industrial meters located in the HAN are summarized under the term "CLS".
▸Section 1.4.2, FDP_IFF.1 application note, document wide	The physical interfaces HAN-CLS and HAN-CON are introduced. The terms IF_GW_* for logical interfaces are no longer in use. Physically separated ports for WAN, LMN, HAN-CLS and HAN-CON are required.
▸Section 1.4.5	The TOE designs describing the design of "A Gateway and multiple Meters" as well as "One Box Solution" were removed.
▸Section 1.4.5	A section has been added to address second source strategies for hardware components.
▸Section 1.4.6, ▸Section 3.5, ▸Section 4.1, ▸FCS_CKM.1/SERVICE	The TOE offers a new security feature, the key generation service for meters and CLS devices.
▸Section 1.4.6, Application note	The TOE allows for the distribution of software updates for devices in the LMN and CLS devices that have been introduced by the GWA. If this functionality is implemented in the TOE, it has to be modelled accordingly in the ST.
▸Section 1.1, ▸Section 1.4.6, ▸Section 7.2	A functional package has been added that models the functionality to control CLS devices with knowledge of the TOE. This functionality is not mandatory to claim strict conformance to the PP. However, if this functionality is implemented in the TOE, the ST has to claim conformance to the functional package.
▸Section 1.4.6, ▸Section 4.1, ▸FMT_MOF.1	Management functionalities for the GWA and for other external entities have been reworked/added. In particular, the SRV has management functionalities for WAN communication parameters. Further management functionalities include but are not limited to: usage of key generation service, change of consumer password, usage of user data reset.
▸Section 1.4.6	The detailed description of the wake-up functionality has been removed. It is instead referred to [BSI-TR-03109-1].
▸Section 1.4.6, ▸Section 4.1, ▸FMT_MOF.1, ▸FMT_MTD.1	The TOE offers a new functionality as part of the security feature "privacy", the user data reset. This functionality shall in particular be used prior to a de- and subsequent re-installation of the TOE.
▸FDP_ACF.1 ▸FIA_UAU.1 ▸FIA_UID.1	The TOE offers a new functionality, a time server for devices in the LMN and HAN. The respective access rules have been updated. FIA_UAU.2 has been replaced by FIA_UAU.1; FIA_UID.2 has been replaced by FIA_UID.1 as the time service of the TOE requires neither authorization nor identification.

Reference in v2.0	Changes in comparison to v1.3
▸Section 1.4.6, ▸Section 6.5.5, FMT_SMF.1 table	The consumer is allowed to change their own password. This has been added as management functionality. The password shall not be stored in plain text.
▸Section 1.4.8	The table depicting the cryptographic support of TOE and security module has been updated and editorial changes have been made. An application note concerning the storage of further keys in the security module and concerning the optional decryption using CMS have been added.
▸Section 1.4.8, FCS_CKM, FTP_PRO.*/CMS	CMS is no longer mandatory for all transmission of meter data to the WAN but only if these data are sent via the GWA to the intended recipient (an EMT).
▸Section 1.4.8	The figure depicting the cryptographic workflow for meter, SMGW and security module has been removed.
▸Section 1.4.9	In the lifecycle description, the phases "delivery to the MPO" and "delivery by the MPO" as well as "de-installation" have been added. It has been addressed that a reusage of the TOE is allowed.
▸Section 1.4.9, ▸Section 3.3, ▸Section 4.2	Adjustment: The part of the delivery that is performed by and under responsibility of the MPO is declared as out of scope of the evaluation and certification. The MPO is assumed to perform this delivery according to the security needs. The MPO is considered trustworthy and sufficiently skilled in context of the delivery.
▸Section 3.1, ▸Glossary	The external entities have been reworked. The consumer has been clarified as natural or legal entity. The SRV has been clarified as local instantiation of the GWA. EMT, meter, CLS and MPO have been added.
▸Section 3.2, ▸Glossary	The assets have been reworked. Assets have been grouped where a distinction is not necessary (e.g., meter data), and new assets have been added (such as HAN device key pair). Existing assets have been reworked (e.g., processing profiles and communication profiles are separate assets).
▸Section 3.3, ▸Section 4.2	Adjustment: The TOE may be installed either in a closed facility with restricted access or in a public environment within a casing. In the latter scenario, the asset PII must not be present on the TOE. This allows for the installation of SMGW in charging stations, distribution boxes or in the depot of the MPO.
▸Section 3.1, ▸Section 3.3, ▸Section 4.2	The term "meter" has been divided into industrial and residential meters. Data generated by industrial meters are not considered PII. Industrial meters are allowed to have an additional unidirectional outbound interface. Residential meters may only be located in the LMN. Industrial meters may be located in the LMN or HAN. In the latter case, the data transmitted from the industrial meters to the TOE are not considered to be meter data.
▸Section 3.3, ▸Section 4.2	A certification according to [BSI-TR-03109-5] is sufficient for the assumption, that a device in the HAN is "appropriately protected", to hold.
▸Section 3.3, ▸Section 4.2	It is additionally assumed that wired connections are connected properly to prevent non-reachability of the TOE due to false-connections of WAN and HAN interfaces.
▸Section 3.5, ▸Section 4.2	Adjustment: It is permitted to continue to use the TOE (after installation) even if the certificate of the security module expires.
▸Section 3.5, ▸Section 4.1, FAU_*/CAL	Adjustment: The data of the calibration log need not be kept on the TOE for the lifetime of the TOE. A deletion of certain events by the GWA or by the SRV is permitted provided that they exported the data beforehand and store them outside the TOE to ensure the required availability of said data according to national regulations concerning the retention period.
▸Section 3.4	The local attacker has been described in more detail.
▸Section 4.3 ▸Section 6.11	The mappings and rationales for the mappings have been reworked and updated.
FAU_GEN.1/SYS	The audit level was adjusted to be "not specified" and a table containing the required auditable events has been added.
FAU_GEN.1/CON	The information, that data in the consumer log have to be kept for 15 months, has been added.
-	The SFR FCO_NRO.2 has been removed.

Reference in v2.0	Changes in comparison to v1.3
FCS_*/* FTP_PRO	The [CC:2022] introduce the new family FTP_PRO trusted channel protocol. These SFRs are used in the PP to model the secure communication with external entities using three iterations FTP_PRO.*/TLS12, FTP_PRO.*/SYM and FTP_PRO.*/CMS. The SFRs FTP_ITC.1/* and FIA_UAU.6 have been removed in this context.
FTP_PRO.*/TLS13	TLSv1.3 is not mandatory to be implemented in the TOE. Optional SFRs modelling TLSv1.3 have been added to be used in an ST if necessary.
FCS_CKM.5/*	The crypto-SFRs of family FCS_CKM have been reworked. They now model the basic methods and mechanisms used for the protocols: FCS_CKM.5/TLS for derivation of write MAC and encryption keys for TLSv1.2. (Optionally TLSv1.3). FCS_CKM.5/CMAC for derivation of MAC and encryption keys for sym meter communication. FCS_CKM.5/X963 for derivation of KEK for CMS.
FCS_COP.1/*	Most crypto-SFRs of family FCS_COP have been reworked. They now model the basic methods and mechanisms used for the protocols: FCS_COP.1/AES for AES in CBC, GCM and CCM mode. FCS_COP.1/HMAC for usage of HMAC in TLSv1.2. FCS_COP.1/CMSCMAC for usage of CMAC in CMS. FCS_COP.1/MTRCMAC for usage of CMAC in communication based on symmetric encryption. FCS_COP.1/AESWRAP for key encryption (AES key wrap) for CMS. FCS_COP.1/HASH and FCS_COP.1/MEM are unchanged except for editorial adjustments.
FDP_IFC, FDP_IFF	The previous meter SFP and Firewall SFP have been merged into one SMGW information flow SFP.
FDP_ACC, FDP_ACF	A table has been added that lists the subjects (i.e., external entities) and the objects they have access to with the kind of access. In addition, the interface via which access is possible is listed. For write/management access, it is referred to the table for FMT_MOF.1.
FIA_UAU.5	SFR has been adjusted for precise usage.
-	FMT_MSA.3/* have been removed as the static attributes of the respective SFPs are set and not changeable.
FMT_SMF.1 table	The management functionalities as described in [CC:2022] Part 2 are suggestions. As such, a rationale for missing management functionality is not necessary in the PP. These rationales have been removed. The management functionalities of new/changed SFRs have been added/reworked.
FMT_MOF.1 table	The table has been updated to describe the management functionalities accessible by the respective roles.
FPT_STM.1	A refinement as per [CC:2022] Part 2 appendix has been added.
FPT_STM.2	This new SFR has been added to model the time source of the TOE and the management of this time source by the GWA. Information was added, that for initial connection establishments to the GWA for NTP purposes, the temporal TLS validity check may be skipped.
▸Table 6.13	The justification for missing dependencies of the SFRs has been included in the dependency table.
▸Section 6.10	Refinements for SARs have been added.

Table B.1 Changelog version 1.3 to version 2.0