Security Target

SMGW Version 2.1

1 Version History

Version	Datum	Name	Änderungen
1.7	19.10.2023	C. Miller	Aktualisierung

Contents

1 Introduction

1.1 ST reference

Title:	Security Target, SMGW Version 2.1
Editors:	Power Plus Communications AG
CC-Version:	3.1 Revision 5
Assurance Level:	EAL 4+, augmented by AVA_VAN.5 and ALC_FLR.2
General Status:	Final
Document Version:	1.7
Document Date:	19.10.2023
TOE:	SMGW Version 2.1
Certification ID:	BSI-DSZ-CC-0831-V7-2023

This document contains the security target of the *SMGW Version 2.1.*

This security target claims conformance to the *Smart Meter Gateway* protection profile [PP_GW].

1.2 TOE reference

The TOE described in this security target is the *SMGW Version 2.1.*

The following classifications of the product *"Smart Meter Gateway"* contain the TOE:

- *BPL Smart Meter Gateway* (BPL-SMGW), SMGW-B-2A-111-00
- *ETH Smart Meter Gateway* (ETH-SMGW), SMGW-E-2A-111-00
- *LTE Smart Meter Gateway* (LTE-SMGW), SMGW-J-2A-111-10, SMGW-J-2A-111-30, SMGW-K-2A-111-10 or SMGW-K-2A-111-30
- *G.hn Smart Meter Gateway* (G.hn-SMGW), SMGW-N-2A-111-00
- *LTE450 Smart Meter Gateway* (LTE450-SMGW), SMGW-V-2A-111-20

The TOE comprises the following parts:

- hardware device of the hardware generation 2A according to Table 1, including the TOE's main circuit board, a carrier board, a power-supply unit and a radio module for communication with wireless meter (included in the hardware device "*Smart Meter Gateway"*)

- firmware including software application (loaded into the circuit board)
    - "*SMGW Software Version 2.2.0*", identified by the value 00861-34788

  which comprises of two revision numbers of the underlying version control system for the TOE, where the first part is for the operating system and the second part is for the SMGW application
- manuals
    - „Handbuch für Verbraucher, Smart Meter Gateway" [AGD_Consumer], identified by the SHA-256 hash value e24e25671d2c16224e058247eb5fdfbb1cfdf8bd89de2ee318f99f1f9e776beb
    - „Handbuch für Service-Techniker, Smart Meter Gateway" [AGD_Techniker], identified by the SHA-256 hash value 9966741b00848419339c729cc6bfff6f7bed2ef348e681e0cb04122ece3865d6
    - „Handbuch für Hersteller von Smart-Meter Gateway-Administrations-Software, Smart Meter Gateway" [AGD_GWA], identified by the SHA-256 hash value 43f69e9458e582262a7d2505209e8b0233a4729854c906d4d29200eb92d70f30
    - „Logmeldungen, SMGW " [SMGW_Logging] identified by the SHA-256 hash value f3a935b6ae1713ccdaa02411b377377a8e4f7dfb092a181efe1a6c9a86f17a64
    - „Auslieferungs- und Fertigungsprozeduren, Anhang Sichere Auslieferung" [AGD_SEC], identified by the SHA-256 hash value 17e280428e1602759b7bfa7dbbfde2e8d65ad7d518a96f0ab41a7130a9f38205

The hardware device "*Smart Meter Gateway*" includes a secure module with the product name "*TCOS Smart Meter Security Module Version 1.0 Release 2/P60C144PVE"* which is not part of the TOE but has its own certification id "BSI-DSZ-CC-0957-V2-2016". Moreover, a hard-wired communication adapter is connected to the TOE via [USB] as shown in Figure 3 which is not part of the TOE (but always an inseparable part of the delivered entity). This communication adapter can be either a LTE communication adapter, a LTE450 communication adapter, a BPL [IEEE 1901] communication adapter, a GPRS communication adapter, a CDMA communication adapter, a powerWAN-Ethernet communication adapter, a G.hn [ITU G.hn] communication adapter or an ethernet communication adapter. There might be not every communication adapter available for each Hardware Generation.

The following table shows the different “Smart Meter Gateway” product classifications applied on the case of the product, while not all of them might be part of the TOE:

#	Characteristic	Value	Description
1	Product family	SMGW	each classification of a type start with this value
2		-	*Delimiter*
3	Communication Technology	B	Product Type „BPL Smart Meter Gateway“
		C	Product Type „CDMA Smart Meter Gateway“
		E	Product Type „ETH Smart Meter Gateway“
		G	Product Type „GPRS Smart Meter Gateway“
		L	Product Type „LTE Smart Meter Gateway“
		J	Product Type “LTE Smart Meter Gateway”
		K	Product Type „LTE Smart Meter Gateway“
		P	Product Type „powerWAN-ETH Smart Meter Gateway“
		N	Product Type „G.hn Smart Meter Gateway“
		V	Product Type “LTE450 Smart Meter Gateway”
4		-	*Delimiter*
5	Hardware generation	1A	Identification of hardware generation; version 1.0 of “SMGW Hardware”
		1B	Identification of hardware generation; version 1.0.1 of “SMGW Hardware” (with new power adapter)

#	Characteristic	Value	Description
		2A	Identification of hardware generation; version 2.0 of “SMGW Hardware”
6		-	*Delimiter*
7	HAN Interface	1	Ethernet
8	CLS Interface	1	Ethernet
9	LMN Interface	1	Wireless and wired
10		-	*Delimiter*
11	SIM card type	0	*None*
		1	SIM card assembled at factory and SIM slot
		2	SIM card assembled at factory only
		3	SIM slot only
12	reserved	0	

Table 1: Smart Meter Gateway product classifications

1.3 Introduction

The increasing use of *green energy* and upcoming technologies around e-mobility lead to an increasing demand for functions of a so called smart grid. A smart grid hereby refers to a commodity[1] 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 a certain commodity (definition adopted from [CEN]).

[1] Commodities can be electricity, gas, water or heat which is distributed from its generator to the consumer through a grid (network).

In its vision such a smart grid would allow to invoke consumer devices to regulate the load and availability of resources or energy in the grid, e.g. by using consumer devices to store energy or by triggering the use of energy based upon the current load of the grid[2]. Basic features of such a smart use of energy or resources are already reality. Providers of electricity in Germany, for example, have to offer at least one tariff that has the purpose to motivate the consumer to save energy.

In the past, the production of electricity followed the demand/consumption of the consumers. Considering the strong increase in renewable energy and the production of energy as a side effect in heat generation today, the consumption/demand has to follow the – often externally controlled – production of energy. Similar mechanisms can exist for the gas network to control the feed of biogas or hydrogen based on information submitted by consumer devices.

An essential aspect for all considerations of a smart grid is the so called *Smart Metering System* that meters the consumption or production of certain commodities at the consumers' side and allows sending the information about the consumption or production to external entities, which is then the basis for e. g. billing the consumption or production.

This Security Target defines the security objectives, corresponding requirements and their fulfilment for a Gateway which is the central communication component of such a Smart Metering System (please refer to chapter 1.4.2 for a more detailed overview).

The Target of Evaluation (TOE) that is described in this document is an electronic unit comprising hardware and software/firmware[3] used for collection, storage and provision of Meter Data[4] from one or more Meters of one or multiple commodities.

The Gateway connects a Wide Area Network (WAN) with a Network of Devices of one or more Smart Metering devices (Local Metrological Network, LMN) and the consumer Home Area Network (HAN), which hosts Controllable Local Systems (CLS) and visualization devices. The security functionality of the TOE comprises

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

[2] Please note that such a functionality requires a consent or a contract between the supplier and the consumer, alternatively a regulatory requirement.

[3] For the rest of this document the term “firmware” will be used if the complete firmware ist meant. For the application including its services the term “software” will be used.

[4] Please refer to chapter 3.2 for an exact definition of the term "Meter Data”.

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 availability of the Gateway is not addressed by this ST.

1.4 TOE Overview

1.4.1 Introduction

The TOE as defined in this Security Target is the Gateway in a Smart Metering System. In the following subsections the overall Smart Metering System will be described first and afterwards the Gateway itself.

There are various different vocabularies existing in the area of Smart Grid, Smart Metering and Home Automation. Furthermore, the Common Criteria maintain their own vocabulary. The Protection Profile [PP_GW, chapter 1.3] provides an overview over the most prominent terms used in this Security Target to avoid any bias which is not fully repeated here.

1.4.2 Overview of the Gateway in a Smart Metering System

The following figure provides an overview of the TOE as part of a complete Smart Metering System from a purely functional perspective as used in this ST.[5]

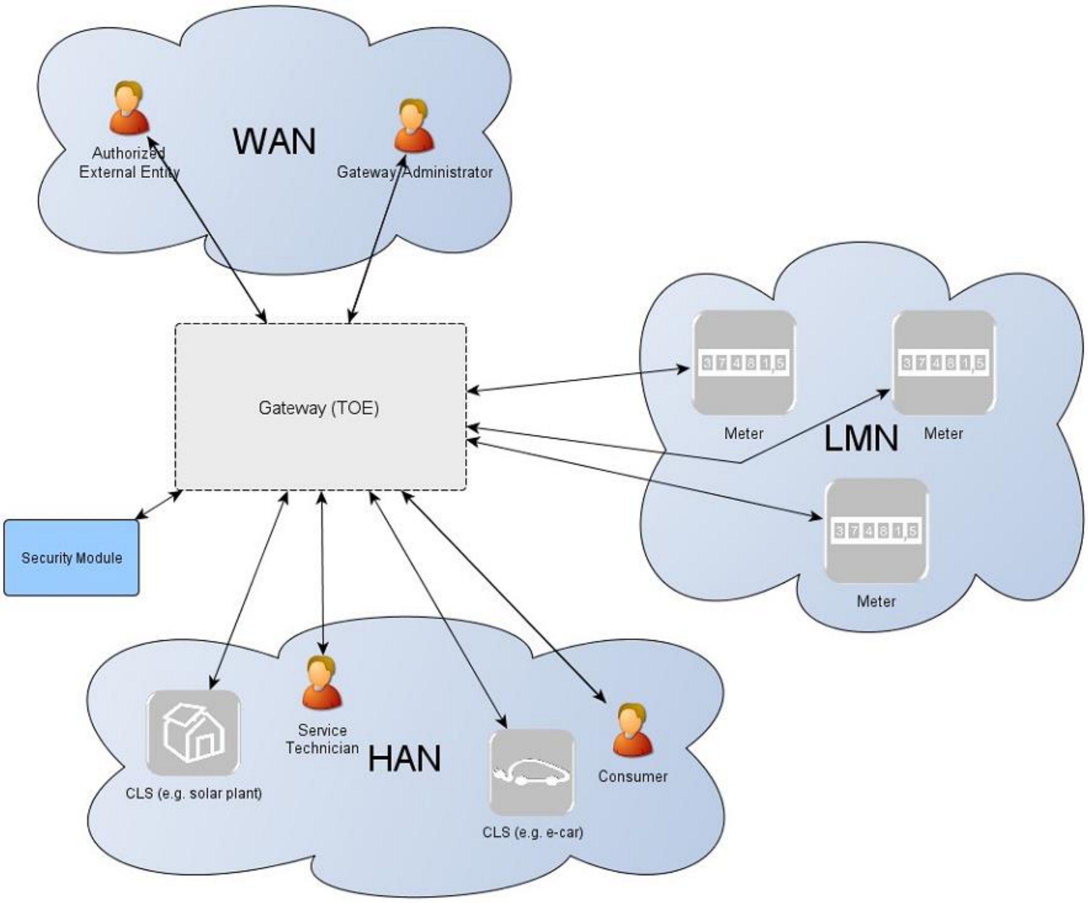

Figure 1: The TOE and its direct environment

As can be seen in Figure 1, a system for smart metering comprises different functional units in the context of the descriptions in this ST:

- The **Gateway** (as defined in this ST) serves as the communication component between the components in the local area network (LAN) of the consumer and the outside world. It can be seen as a special kind of firewall dedicated to the smart metering functionality. It also collects, processes and stores the records

[5] It should be noted that this description purely contains aspects that are relevant to motivate and understand the functionalities of the Gateway as described in this ST. It does not aim to provide a universal description of a Smart Metering System for all application cases.

from Meter(s) and ensures that only authorised parties have access to them or derivatives thereof. Before sending meter data[6] the information will be encrypted and signed using the services of a Security Module. The Gateway features a mandatory user interface, enabling authorised consumers to access the data relevant to them.

- 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 Gateway. The Meter Data has to be signed and encrypted before transfer in order to ensure its confidentiality, authenticity, and integrity. The Meter is comparable to a classical meter[7] 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 Gateway[8].
- The Gateway utilises the services of a **Security Module** (e.g. a smart card) as a cryptographic service provider and as a secure storage for confidential assets. The Security Module will be evaluated separately according to the requirements in the corresponding Protection Profile (c.f. [SecModPP]).

Controllable Local Systems (CLS, as shown in Figure 2) may range from local power generation plants, controllable loads such as air condition and intelligent household appliances (“white goods”) to applications in home automation. CLS may utilise the services of the Gateway for communication services. However, CLS are not part of the Smart Metering System.

The following figure introduces the external interfaces of the TOE and shows the cardinality of the involved entities. Please note that the arrows of the interfaces within the Smart Metering System as shown in Figure 2 indicate the flow of information. However, it does not indicate that a communication flow can be initiated bi-directionally. Indeed,

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

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

[8] It should be noted that this ST does not imply that the connection between the Gateways and external components (specifically meters and CLS) is cable based. It is also possible that the connections as shown in Figure 1 are realised deploying a wireless technology. However, the requirements on how the connections shall be secured apply regardless of the realisation.

the following chapters of this ST will place dedicated requirements on the way an information flow can be initiated[9].

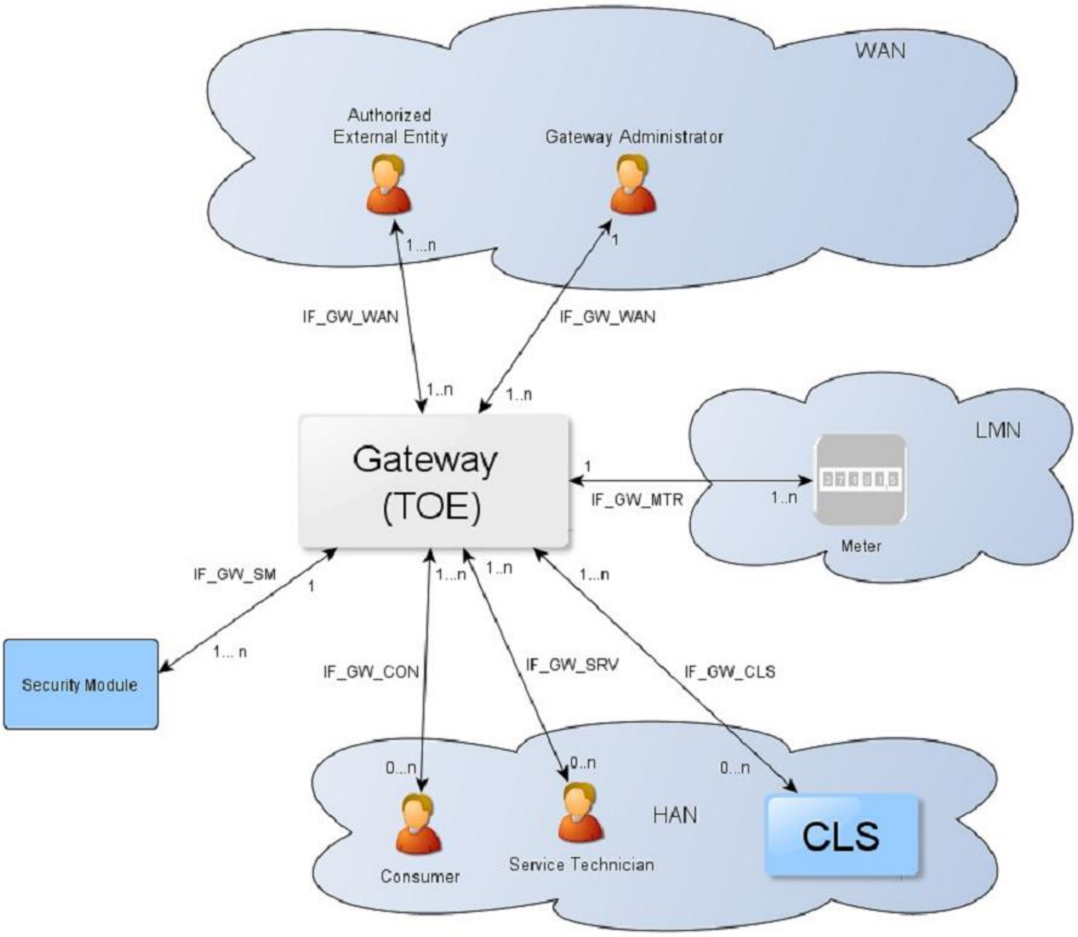

Figure 2: The logical interfaces of the TOE

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 has been motivated by the following considerations:

- The Gateway is the central communication unit in the Smart Metering System. It is the only unit directly connected to the WAN, to be the first line of defence an attacker located in the WAN would have to conquer.
- The Gateway is the central component that collects, processes and stores Meter Data. It therewith is the primary point for user interaction in the context of the Smart Metering System.

[9] Please note that the cardinality of the interface to the consumer is 0...n as it cannot be assumed that a consumer is interacting with the TOE at all.

- To conquer a Meter in the LMN or CLS in the HAN (that uses the TOE for communication) a WAN attacker first would have to attack the Gateway successfully. All data transferred between LAN and WAN flows via the Gateway which makes it an ideal unit for implementing significant parts of the system's overall security functionality.
- Because a Gateway can be used to connect and protect multiple Meters (while a Meter will always be connected to exactly one Gateway) and CLS with the WAN, there might be more Meters and CLS in a Smart Metering System than there are Gateways.

All these arguments motivated the approach to have a Gateway (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.

1.4.3 TOE description

The Smart Metering Gateway (in the following short: Gateway or TOE) may serve as the communication unit between devices of private and commercial consumers and service providers of a commodity industry (e.g. electricity, gas, water, etc.). It also collects, processes and stores Meter Data and is responsible for the distribution of this data to external entities.

Typically, the Gateway will be placed in the household or premises of the consumer[10] of the commodity and enables access to local Meter(s) (i.e. the unit(s) used for measuring the consumption or production of electric power, gas, water, heat etc.) and may enable access to Controllable Local Systems (e.g. power generation plants, controllable loads such as air condition and intelligent household appliances).

The TOE has a fail-safe design that specifically ensures that any malfunction can not impact the delivery of a commodity, e.g. energy, gas or water[11].

[10] Please note that it is possible that the consumer of the commodity is not the owner of the premises where the Gateway will be placed. However, this description acknowledges that there is a certain level of control over the physical access to the Gateway.

[11] Indeed, this Security Target assumes that the Gateway and the Meters have no possibility at all to impact the delivery of a commodity. Even an intentional stop of the delivery of a certain commodity is Not within the scope of this Security Target. It should, however, be noted that such a functionality may be realised by a CLS that utilises the services of the TOE for its communication.

The following figure provides an overview of the product with its TOE and non-TOE parts:

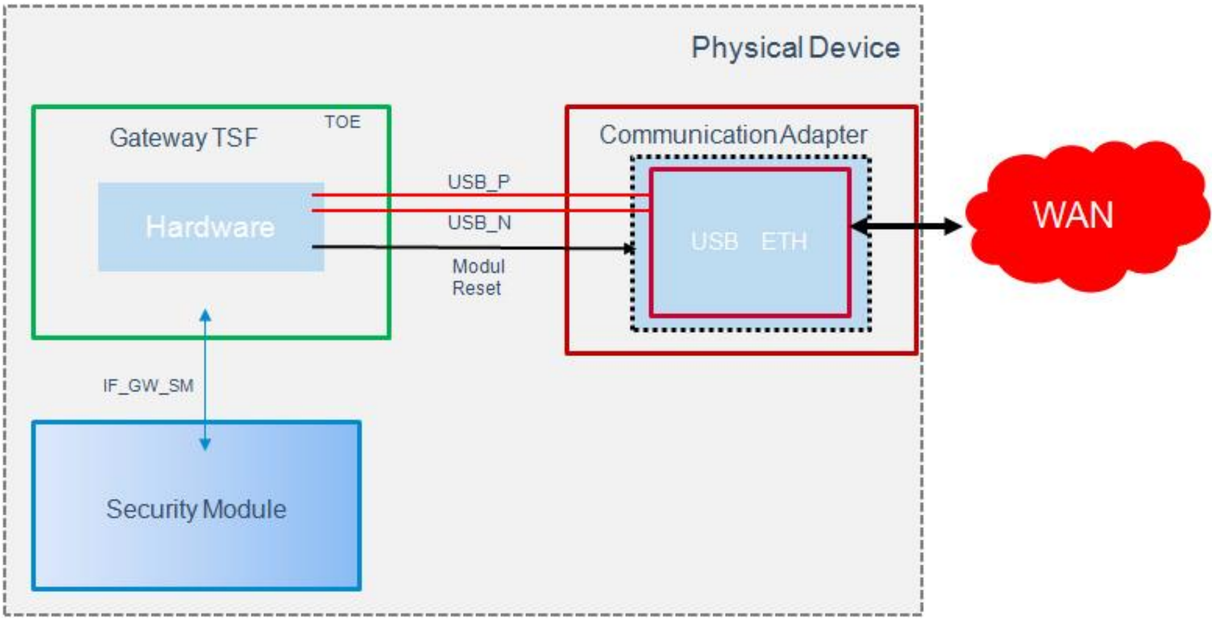

Figure 3: The product with its TOE and non-TOE parts

The TOE communicates over the interface IF_GW_SM with a security module and over the interfaces *USB_P*, *USB_N* and *Module Reset* with one of the possible communication adapters according to chapter 1.2. The communication adapters, which are not part of the TOE, transmit data from the USB interface to the WAN interface and vice versa.

1.4.4 TOE Type definition

At first, 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 is responsible for the distribution of this data to external parties.

Typically, the Gateway will be placed in the household or premises of the consumer of the commodity and enables access to local Meter(s) (i.e. the unit(s) used for measuring the consumption or production of electric power, gas, water, heat etc.) and may enable access to Controllable Local Systems (e.g. power generation plants, controllable loads such as air condition and intelligent household appliances). Roles respectively External Entities in the context of the TOE are introduced in chapter 3.1.

The TOE described in this ST is a product that has been developed by Power Plus Communication AG. It is a communication product which complies with the requirements of the Protection Profile “Protection Profile for the Gateway of a Smart Metering System”

[PP_GW]. The TOE consists of hardware and software including the operating system. The communication with more than one meter is possible.

The TOE is implemented as a separate physical module which can be integrated into more complex modular systems. This means that the TOE can be understood as an OEM module which provides all required physical interfaces and protocols on well defined interfaces. Because of this, the module can be integrated into communication devices and directly into meters.

The TOE-design includes the following components:

- The security relevant components compliant to the Protection Profile.
- Components with no security relevance (e.g. communication protocols and interfaces).

The TOE evaluation does not include the evaluation of the Security Module. In fact, the TOE relies on the security functionality of the Security Module but it must be security evaluated in a separate security evaluation[12].

The hardware platform of the TOE mainly consists of a suitable embedded CPU, volatile and non-volatile memory and supporting circuits like Security Module and RTC.

The TOE contains mechanisms for the integrity protection for its firmware.

The TOE supports the following communication protocols:

- OBIS according to [IEC-62056-6-1] and [EN 13757-1],
- DLMS/COSEM according to [IEC-62056-6-2],
- SML according to [IEC-62056-5-3-8],
- unidirectional and bidirectional wireless M-Bus according to [EN 13757-3], [EN 13757-4], and [IEC-62056-21].

[12] Please note that the Security Module is physically integrated into the Gateway even though it is not part of the TOE.

The TOE provides the following physical interfaces for communication

- Wireless M-Bus (LMN) according to [EN 13757-3],
- RS-485 (LMN) according to [EIA RS-485],
- Ethernet (HAN) according to [IEEE 802.3], and
- USB (WAN) according to [USB].

The physical interface for the WAN communication is described in chapter 1.4.3. The communication is protected according to [TR-03109].

The communication into the HAN is also provided by the Ethernet interface. The protocols HTTPS and TLS proxy are therefore supported.

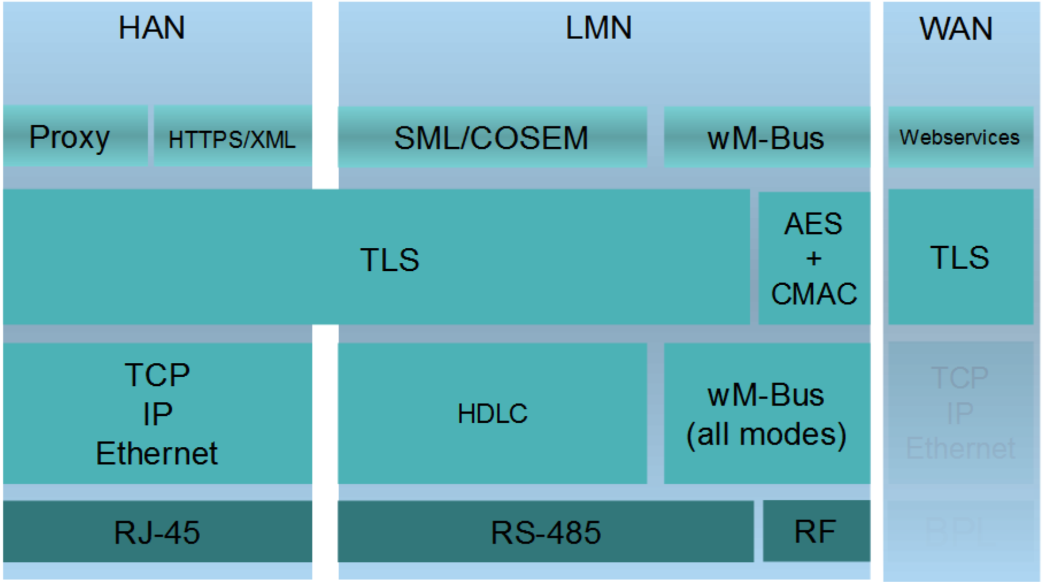

Figure 4: The TOE's protocol stack

The TOE provides the following functionality:

- Protected handling of Meter Data compliant to [PP_GW, chapter 1.4.6.1 and 1.4.6.2]
- Integrity and authenticity protection e. g. of Meter Data compliant to [PP_GW, chapter 1.6.4.3]
- Protection of LAN devices against access from the WAN compliant to [PP_GW, chapter 1.4.6.4]
- Wake-Up Service compliant to [PP_GW, chapter 1.4.6.5]
- Privacy protection compliant to [PP_GW, chapter 1.4.6.6]
- Management of Security Functions compliant to [PP_GW, chapter 1.4.6.7]

- Cryptography of the TOE and its Security Module compliant to [PP_GW, chapter 1.4.8]

1.4.5 TOE logical boundary

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

- *Handling of Meter Data*, collection and processing of Meter Data, submission to authorised external entities (e.g. one of the service providers involved) where necessary protected by a digital signature
- *Protection of authenticity, integrity and confidentiality* of data temporarily or persistently stored in the Gateway, transferred locally within the LAN and transferred in the WAN (between Gateway and authorised external entities)
- *Firewalling* of information flows to the WAN and information flow control among Meters, Controllable Local Systems and the WAN
- A *Wake-Up-Service* that allows to contact the TOE from the WAN side
- *Privacy preservation*
- *Management* of Security Functionality
- *Identification and Authentication* of TOE users

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

1.4.5.1 Handling of Meter Data[13]

The Gateway is responsible for handling Meter Data. It receives the Meter Data from the Meter(s), processes it, stores it and submits it to external entities.

The TOE utilises Processing Profiles to determine which data shall be sent to which component or external entity. A Processing Profile defines:

- how Meter Data must be processed,
- which processed Meter Data must be sent in which intervals,
- to which component or external entity,
- signed using which key material,
- encrypted using which key material,
- whether processed Meter Data shall be pseudonymised or not, and
- which pseudonym shall be used to send the data.

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

The Processing Profiles are not only the basis for the security features of the TOE; they also contain functional aspects as they indicate to the Gateway how the Meter Data shall be processed. More details on the Processing Profiles can be found in [TR-03109-1].

The Gateway restricts access to (processed) Meter Data in the following ways:

- consumers must be identified and authenticated first before access to any data may be granted,
- the Gateway accepts Meter Data from authorised Meters only,
- the Gateway sends processed Meter Data to correspondingly authorised external entities only.

The Gateway accepts data (e.g. configuration data, firmware updates) from correspondingly authorised Gateway Administrators or correspondingly authorised external entities only. This restriction is a prerequisite for a secure operation and therewith for a secure handling of Meter Data. Further, the Gateway maintains a calibration log with all relevant events that could affect the calibration of the Gateway.

These functionalities:

- prevent that the Gateway accepts data from or sends data to unauthorised entities,
- ensure that only the minimum amount of data leaves the scope of control of the consumer,
- preserve the integrity of billing processes and as such serve in the interests of the consumer as well as in the interests of the supplier. Both parties are interested in an billing process that ensures that the value of the consumed amount of a certain commodity (and only the used amount) is transmitted,
- preserve the integrity of the system components and their configurations.

The TOE offers a local interface to the consumer (see also IF_GW_CON in Figure 2) and allows the consumer to obtain information via this interface. 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 entity. The TOE ensures that the communication to the consumer is protected by using TLS and ensures that consumers only get access to their own data. Therefore, the TOE contains a web server that delivers the content to the web browser after successful authentication of the user.

1.4.5.2 Confidentiality protection

The TOE protects data from unauthorised disclosure

- while received from a Meter via the LMN,
- while received from the administrator via the WAN,
- while temporarily stored in the volatile memory of the Gateway,
- while transmitted to the corresponding external entity via the WAN or HAN.

Furthermore, all data, which no longer have to be stored in the Gateway, are securely erased to prevent any form of access to residual data via external interfaces of the TOE. These functionalities protect the privacy of the consumer and prevent that an unauthorised party is able to disclose any of the data transferred in and from the Smart Metering System (e.g. Meter Data, configuration settings).

The TOE utilises the services of its Security Module for aspects of this functionality.

1.4.5.3 Integrity and Authenticity protection

The Gateway provides 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. The TOE utilises the services of its Security Module for aspects of this functionality.
- Application of authenticity and integrity protection measures when sending processed Meter Data to an external entity, to enable the external entity to verify that the processed Meter Data have been sent from an authentic Gateway and have not been changed during transmission. The TOE utilises the services of its Security Module for aspects of this functionality.
- 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 authorised external entity and have not been changed during transmission. The TOE utilises the services of its Security Module for aspects of this functionality.

These functionalities

- 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 billing processes and serve for the interests of the consumer as well as for the interest of the supplier. Both parties are interested in the transmission of correct processed Meter Data to be used for billing,
- 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 in the system.

1.4.5.4 Information flow control and firewall

The Gateway separates devices in the LAN of the consumer from the WAN and enforces the following information flow control to control the communication between the networks that the Gateway is attached to:

- only the Gateway may establish a connection to an external entity in the WAN[14]; specifically connection establishment by an external entity in the WAN or a Meter in the LMN to the WAN is not possible,
- the Gateway can establish connections to devices in the LMN or in the HAN,
- Meters in the LMN are only allowed to establish a connection to the Gateway,
- the Gateway shall offer a wake-up service that allows external entities in the WAN to trigger a connection establishment by the Gateway,
- connections are allowed to pre-configured addresses only,
- only cryptographically-protected (i.e. encrypted, integrity protected and mutually authenticated) connections are possible.[15]

These functionalities

- prevent that the Gateway itself or the components behind the Gateway (i.e. Meters or Controllable Local Systems) can be conquered by a WAN attacker (as defined in section 3.4), that processed data are transmitted to the wrong external entity, and that processed data are transmitted without being confidentiality/authenticity/integrity-protected,
- protect the Smart Metering System and a corresponding large scale infrastructure in two ways: by preventing that conquered components will send forged

[14] Please note that this does not affect the functionality for a CLS to establish a secure channel to a party in the WAN. Technically however, this channel is established by the TOE who acts as a proxy between the CLS and the WAN.

[15] 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 or LAN is allowed.

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/firmware to attack other systems in the WAN (e.g. a WAN attacker who would be able to install a botnet on components of the Smart Metering System).

The communication flows that are enforced by the Gateway between parties in the HAN, LMN and WAN are summarized in the following table[16]:

Source(1st column) **Destination (1st row)**	**WAN**	**LMN**	**HAN**
WAN	- (see following list)	No connection establishment allowed	No connection establishment allowed
LMN	No connection establishment allowed	- (see following list)	No connection establishment allowed
HAN	Connection establishment is allowed to trustworthy, pre-configured endpoints and via an encrypted channel only[17]	No connection establishment allowed	- (see following list)

Table 2: Communication flows between devices in different networks

For communications within the different networks the following assumptions are defined:

1. Communications within the **WAN** are not restricted. However, the Gateway is not involved in this communication,
2. No communications between devices in the **LMN** are assumed. Devices in the LMN may only communicate to the Gateway and shall not be connected to any other network,
3. Devices in the **HAN** may communicate with each other. However, the Gateway is not involved in this communication. If devices in the HAN have a separate

[16] Please note that this table only addresses the communication flow between devices in the various networks attached to the Gateway. It does not aim to provide an overview over the services that the Gateway itself offers to those devices nor an overview over the communication between devices in the same network. This information can be found in the paragraphs following the table.

[17] The channel to the external entity in the WAN is established by the Gateway.

connection to parties in the WAN (beside the Gateway) this connection is assumed to be appropriately protected. It should be noted that for the case that a TOE connects to more than one HAN communications between devices within different HAN via the TOE are only allowed if explicitly configured by a Gateway Administrator.

Finally, the Gateway itself offers the following services within the various networks:

- the Gateway accepts the submission of Meter Data from the LMN,
- the Gateway offers a wake-up service at the WAN side as described in chapter 1.4.6.5 of [PP_GW],
- the Gateway offers a user interface to the HAN that allows CLS or consumers to connect to the Gateway in order to read relevant information.

1.4.5.5 Wake-Up-Service

In order to protect the Gateway and the devices in the LAN against threats from the WAN side the Gateway implements a strict firewall policy and enforces that connections with external entities in the WAN shall only be established by the Gateway itself (e.g. when the Gateway delivers Meter Data or contacts the Gateway Administrator to check for updates)[18].

While this policy is the optimal policy from a security perspective, the Gateway Administrator may want to facilitate applications in which an instant communication to the Gateway is required.

In order to allow this kind of re-activeness of the Gateway, this ST allows the Gateway to keep existing connections to external entities open (please refer to [TR-03109-3] for more details) and to offer a so called wake-up service.

The Gateway is able to receive a wake-up message that is signed by the Gateway Administrator. The following steps are taken:

1. The Gateway verifies the wake-up packet. This comprises
   i. a check if the header identification is correct,
   ii. the recipient is the Gateway,
   iii. the wake-up packet has been sent/received within an acceptable period of time in order to prevent replayed messages,

[18] Please note that this does not affect the functionality for a CLS to establish a secure channel to a party in the WAN. Technically however, this channel is established by the TOE who acts as a proxy between the CLS and the WAN.

   iv. the wake-up message has not been received before,

2. If the wake-up message could not be verified as described in step #1, the message will be dropped/ignored. No further operations will be initiated and no feedback is provided.
3. If the message could be verified as described in step #1, the signature of the wake-up message will be verified. The Gateway uses the services of its Security Module for signature verification.
4. If the signature of the wake-up message cannot be verified as described in step #3 the message will be dropped/ignored. No feedback is given to the sending external entity and the wake-up sequence terminates.
5. If the signature of the wake-up message could be verified successfully , the Gateway initiates a connection to a pre-configured external entity; however no feedback is given to the sending external entity.

More details on the exact implementation of this mechanism can be found in [TR-03109-1, „Wake-Up Service“].

1.4.5.6 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 ST.

This contains two aspects:

The Processing Profiles that the TOE obeys facilitate an approach in which only a minimum amount of data have to be submitted to external entities and therewith leave the scope of control of the consumer. The mechanisms “encryption” and “pseudonymisation” ensure that the data can only be read by the intended recipient and only contains an association with the identity of the Meter if this is necessary.

On the other hand, the TOE provides the consumer with transparent information about the information flows that happen with their data. In order to achieve this, the TOE implements a consumer log that specifically contains the information about the information flows which has been and will be authorised based on the previous and current Processing Profiles. The access to this consumer log is only possible via a local interface from the HAN and after authentication of the consumer. The TOE does only allow a consumer access to the data in the consumer log that is related to their own consumption or production. The following paragraphs provide more details on the information that is included in this log:

Monitoring of Data Transfers

The TOE keeps track of each data transmission in the consumer log and allows the consumer to see details on which information have been and will be sent (based on the previous and current settings) to which external entity.

Configuration Reporting

The TOE provides detailed and complete reporting in the consumer log of each security and privacy-relevant configuration setting. Additional to device specific configuration settings, the consumer log contains the parameters of each Processing Profile. The consumer log contains the configured addresses for internal and external entities including the CLS.

Audit Log and Monitoring

The TOE provides all audit data from the consumer log at the user interface IF_GW_CON. Access to the consumer log is only possible after successful authentication and only to information that the consumer has permission to (i.e. that has been recorded based on events belonging to the consumer).

1.4.5.7 Management of Security Functions

The Gateway provides authorised Gateway Administrators with functionality to manage the behaviour of the security functions and to update the TOE.

Further, it is defined that only authorised Gateway Administrators may be able to use the management functionality of the Gateway (while the Security Module is used for the authentication of the Gateway Administrator) and that the management of the Gateway shall only be possible from the WAN side interface.

System Status

The TOE provides information on the current status of the TOE in the system log. Specifically it shall indicate whether the TOE operates normally or any errors have been detected that are of relevance for the administrator.

1.4.5.8 Identification and Authentication

To protect the TSF as well as User Data and TSF data from unauthorized modification the TOE provides a mechanism that requires each user to be successfully identified and authenticated before allowing any other actions on behalf of that user. This functionality includes the identification and authentication of users who receive data from the

Gateway as well as the identification and authentication of CLS located in HAN and Meters located in LMN.

The Gateway provides different kinds of identification and authentication mechanisms that depend on the user role and the used interfaces. Most of the mechanisms require the usage of certificates. Only consumers are able to decide whether they use certificates or username and password for identification and authentication.

1.4.6 The logical interfaces of the TOE

The TOE offers its functionality as outlined before via a set of external interfaces. Figure 2 also indicates the cardinality of the interfaces. The following table provides an overview of the mandatory external interfaces of the TOE and provides additional information:

Interface Name	**Description**
IF_GW_CON	Via this interface the Gateway provides the consumer[19] with the possibility to review information that is relevant for billing or the privacy of the consumer. Specifically the access to the consumer log is only allowed via this interface.
IF_GW_MTR	Interface between the Meter and the Gateway. The Gateway receives Meter Data via this interface.[20]
IF_GW_SM	The Gateway invokes the services of its Security Module via this interface.
IF_GW_CLS	CLS may use the communication services of the Gateway via this interface. The implementation of at least one interface for CLS is mandatory.
IF_GW_WAN	The Gateway submits information to authorised external entities via this interface.
IF_GW_SRV	Local interface via which the service technician has the possibility to review information that are relevant to maintain the Gateway. Specifically he has

[19] Please note that this interface allows consumer (or consumer’s CLS) to connect to the gateway in order to read consumer specific information.

[20] Please note that an implementation of this external interface is also required in the case that Meter and Gateway are implemented within one physical device in order to allow the extension of the system by another Meter.

	read access to the system log only via this interface. He has also the possibility to view non-TSF data via this interface.

Table 3: Mandatory TOE external interfaces

1.4.7 The cryptography of the TOE and its Security Module

Parts of the cryptographic functionality used in the upper mentioned functions is 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 Gateway Administrator. The Security Module is a different IT product and not part of the TOE as described in this ST. Nevertheless, it is physically embedded into the Gateway and protected by the same level of physical protection. The requirements applicable to the Security Module are specified in a separate PP (see [SecModPP]).

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 entities	• encryption • decryption • hashing • key derivation • MAC generation • MAC verification • secure storage of the TLS certificates	Key negotiation: • support of the authentication of the external entity • secure storage of the private key • random number generation • digital signature verification and generation
Communicationwith the consumer	• encryption • decryption • hashing • key derivation • MAC generation • MAC verification • secure storage of the TLS certificates	Key negotiation: • support of the authentication of the consumer • secure storage of the private key • digital signature verification and generation • random number generation

Communication with the Meter	• encryption • decryption • hashing • key derivation • MAC generation • MAC verification • secure storage of the TLS certificates	Key negotiation (in case of TLS connection): • support of the authentication of the meter • secure storage of the private key • digital signature verification and generation • random number generation
Signing data before submission to an external entity	• hashing	Signature creation • secure storage of the private key
Content data encryption and integrity protection	• encryption • decryption • MAC generation • key derivation • secure storage of the public Key	Key negotiation: • secure storage of the private key • random number generation

Table 4: Cryptographic support of the TOE and its Security Module

1.4.7.1 Content data encryption vs. an encrypted channel

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

As a general rule, all processed Meter Data that is prepared to be submitted to external entities is encrypted and integrity protected on a content level using CMS (according to [TR-03109-1-I]).

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

This concept of encryption on two layers facilitates use cases in which the external party that the TOE communicates with is not the final recipient of the Meter Data. In this way, it is for example possible that the Gateway Administrator receives Meter Data that they forward to other parties. In such a case, the Gateway Administrator is the endpoint of the trusted channel but cannot read the Meter Data.

Administration data that is transmitted between the Gateway Administrator and the TOE is also encrypted and integrity protected using CMS.

The following figure introduces the communication process between the Meter, the TOE and external entities (focussing on billing-relevant Meter Data).

The basic information flow for Meter Data is as follows and shown in Figure 5:

1. The Meter measures the consumption or production of a certain commodity.
2. The Meter Data is prepared for transmission:
   a. The Meter Data is typically signed (typically using the services of an integrated Security Module).
   b. If the communication between the Meter and the Gateway is performed bidirectional, the Meter Data is transmitted via an encrypted and mutually authenticated channel to the Gateway. Please note that the submission of this information may be triggered by the Meter or the Gateway.

   or

   c. If a unidirectional communication is performed between the Meter and the Gateway, the Meter Data is encrypted using a symmetric algorithm (according to [TR-03109-3]) and facilitating a defined data structure to ensure the authenticity and confidentiality.
3. The authenticity and integrity of the Meter Data is verified by the Gateway.
4. If (and only if) authenticity and integrity have been verified successfully, the Meter Data is further processed by the Gateway according to the rules in the Processing Profile else the cryptographic information flow will be cancelled.
5. The processed Meter Data is encrypted and integrity protected using CMS (according to [TR-03109-1-I]) for the final recipient of the data[21].
6. The processed Meter Data is signed using the services of the Security Module.
7. The processed and signed Meter Data may be stored for a certain amount of time.

[21] Optionally the Meter Data can additionally be signed before any encryption is done.

8. The processed Meter Data is finally submitted to an authorised external entity in the WAN via an encrypted and mutually authenticated channel.

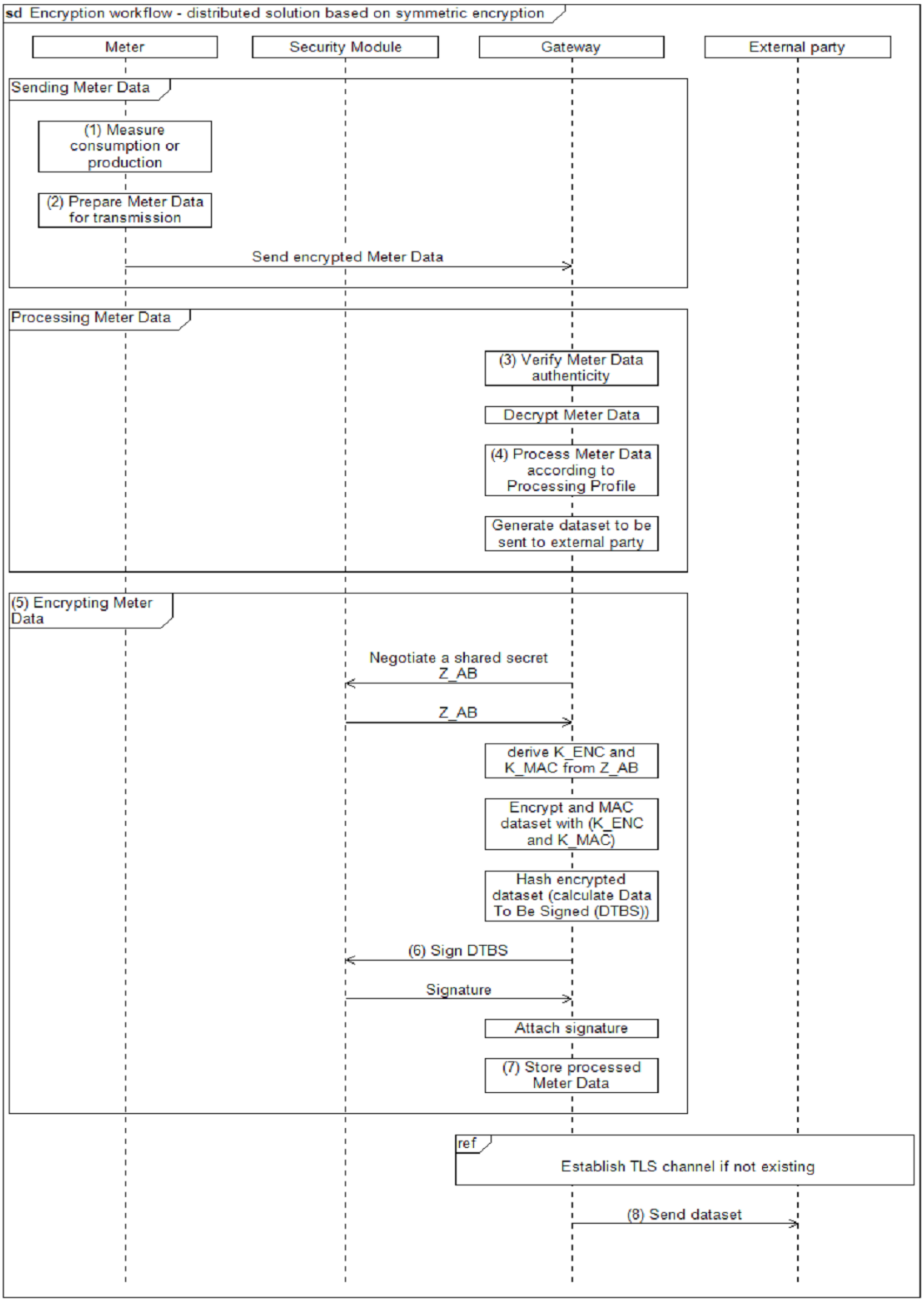
sd Encryption workflow - distributed solution based on symmetric encryption
Meter
Security Module
Gateway
External party
Sending Meter Data
(1) Measure consumption or production
(2) Prepare Meter Data for transmission
Send encrypted Meter Data
Processing Meter Data
(3) Verify Meter Data authenticity
Decrypt Meter Data
(4) Process Meter Data according to Processing Profile
Generate dataset to be sent to external party
(5) Encrypting Meter Data
Negotiate a shared secret Z_AB
Z_AB
derive K_ENC and K_MAC from Z_AB
Encrypt and MAC dataset with (K_ENC and K_MAC)
Hash encrypted dataset (calculate Data To Be Signed (DTBS))
(6) Sign DTBS
Signature
Attach signature
(7) Store processed Meter Data
ref
Establish TLS channel if not existing
(8) Send dataset

Figure 5: Cryptographic information flow for distributed Meters and Gateway

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. Installation and start of operation
6. Personalization
7. Normal operation

A detailed description of the phases #1 to #4 and #6 to #7 is provided in [TR-03109-1-VI], while phase #5 is described in the TOE manuals.

The TOE will be delivered after phase “Pre-personalization and integration of Security Module”. The phase “Personalization” will be performed when the TOE is started for the first time after phase “Installation and start of operation”. The TOE delivery process is specified in [AGD_SEC].

2 Conformance Claims

2.1 CC Conformance Claim

- This ST has been developed using Version 3.1 Revision 5 of Common Criteria [CC].
- This ST is [CC] part 2 extended due to the use of FPR_CON.1.
- This ST claims conformance to [CC] part 3; no extended assurance components have been defined.

2.2 PP Claim / Conformance Statement

This Security Target claims strict conformance to Protection Profile [PP_GW].

2.3 Package Claim

This Security Target claims an assurance package EAL4 augmented by AVA_VAN.5 and ALC_FLR.2 as defined in [CC] Part 3 for product certification.

2.4 Conformance Claim Rationale

This Security Target claims strict conformance to only one PP [PP_GW].

This Security Target is consistent to the TOE type according to [PP_GW] because the TOE is a communication Gateway that 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.

This Security Target is consistent to the security problem defined in [PP_GW].

This Security Target is consistent to the security objectives stated in [PP_GW], no security objective of the PP is removed, nor added to this Security Target.

This Security Target is consistent to the security requirements stated in [PP_GW], no security requirement of the PP is removed, nor added to this Security Target.

3 Security Problem Definition

3.1 External entities

The following external entities interact with the system consisting of Meter and Gateway. Those roles have been defined for the use in this Security Target. It is possible that a party implements more than one role in practice.

Role	**Description**
Consumer	The authorised individual or organization that "owns" the Meter Data. 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).
Gateway Administrator	Authority that installs, configures, monitors, and controls the Smart Meter Gateway.
Service Technician	The authorised individual that is responsible for diagnostic purposes.
Authorised External Entity / User	Human or IT entity possibly interacting with the TOE from outside of the TOE boundary. In the context of this ST, the term *user* or *external entity* serve as a hypernym for all entities mentioned before.

Table 5: Roles used in the Security Target

3.2 Assets

The following tables introduces the relevant assets for this Security Target. The tables focus on the assets that are relevant for the Gateway and does not claim to provide an overview over all assets in the Smart Metering System or for other devices in the LMN.

The following Table 6 lists all assets typified as "user data":

Asset	Description	Need for Protection
Meter Data	Meter readings that allow calculation of the quantity of a commodity, e.g. electricity, gas, water or heat consumed over a period. Meter Data comprise Consumption or Production Data (billing-relevant) and grid status data (not billing-relevant). While billing-relevant data needs to have a relation to the Consumer, grid status data do not have to be directly related to a Consumer.	• According to their specific need (see below)
System log data	Log data from the • system log.	• Integrity • Confidentiality (only authorised SMGW administrators and Service technicians may read the log data)
Consumer log data	Log data from the • consumer log.	• Integrity • Confidentiality (only authorised Consumers may read the log data)
Calibration log data	Log data from the • calibration log.	• Integrity • Confidentiality (only authorised SMGW administrators may read the log data)
Consumption Data	Billing-relevant part of Meter Data. Please note that the term *Consumption Data* implicitly includes Production Data.	• Integrity and authenticity (comparable to the classical meter and its security requirements) • Confidentiality (due to privacy concerns)

Status Data	Grid status data, subset of Meter Data that is not billing-relevant[22].	• Integrity and authenticity (comparable to the classical meter and its security requirements) • Confidentiality (due to privacy concerns)
Supplementary Data	The Gateway may be used for communication purposes by devices in the LMN or HAN. It may be that the functionality of the Gateway that is used by such a device is limited to pure (but secure) communication services. Data that is transmitted via the Gateway but that does not belong to one of the aforementioned data types is named *Supplementary Data*.	• According to their specific need
Data	The term *Data* is used as hypernym for *Meter Data and Supplementary Data*.	• According to their specific need
Gateway time	Date and time of the real-time clock of the Gateway. Gateway Time is used in Meter Data records sent to external entities.	• Integrity • Authenticity (when time is adjusted to an external reference time)
Personally Identifiable Information (PII)	Personally Identifiable Information refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.	• Confidentiality

722 **Table 6: Assets (User data)**

723 Table 7 lists all assets typified as "TSF data":

[22] Please note that these readings and data of the Meter which are not relevant for billing may require an explicit endorsement of the consumer(s).

Asset	Description	Need for Protection
Meter config (secondary asset)	Configuration data of the Meter to control its behaviour including the Meter identity. Configuration data is transmitted to the Meter via the Gateway.	• Integrity and authenticity • Confidentiality
Gateway config (secondary asset)	Configuration data of the Gateway to control its behaviour including the Gateway identity, the Processing Profiles and certificate/key material for authentication.	• Integrity and authenticity • Confidentiality
CLS config (secondary asset)	Configuration data of a CLS to control its behaviour. Configuration data is transmitted to the CLS via the Gateway.	• Integrity and authenticity • Confidentiality
Firmware update (secondary asset)	Firmware update that is downloaded by the TOE to update the firmware of the TOE.	• Integrity and authenticity
Ephemeral keys (secondary asset)	Ephemeral cryptographic material used by the TOE for cryptographic operations.	• Integrity and authenticity • Confidentiality

724 **Table 7: Assets (TSF data)**

725

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 authorised 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 unauthorised analyses of this data with respect to the corresponding Consumer(s).

A.TrustedAdmins It is assumed that the Gateway Administrator and the Service Technician are trustworthy and well-trained.

A.PhysicalProtection It is assumed that the TOE is installed in a non-public environment within the premises of the Consumer which provides a basic level of physical protection. This protection covers the TOE, the Meter(s) that the TOE communicates with and the communication channel between the TOE and its Security Module.

A.ProcessProfile The Processing Profiles that are used when handling data are assumed to be trustworthy and correct.

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

A.Network It is assumed that

- a WAN network connection with a sufficient reliability and bandwidth for the individual situation is available,
- one or more trustworthy sources for an update of the system time are available in the WAN,

- the Gateway is the only communication gateway for Meters in the LMN[23],
- if devices in the HAN have a separate connection to parties in the WAN (beside the Gateway) this connection is appropriately protected.

A.Keygen It is assumed that the ECC key pair for a Meter (TLS) is generated securely according to [TR-03109-3] and brought into the Gateway in a secure way by the Gateway Administrator.

Application Note 1: This ST acknowledges that the Gateway cannot be completely protected against unauthorised physical access by its environment. However, it is important for the overall security of the TOE that it is not installed within a public environment.

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 [TR-03109-1].

Application Note 2: The Processing Profiles that are used for information flow control as referred to by A.ProcessProfile 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, e.g. whether the data needs to be related to the Consumer (because it is used for billing purposes) or whether the data shall be pseudonymised.

The Processing Profiles shall be visible for the Consumer to allow a transparent communication.

[23] Please note that this assumption 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. This is specifically true for wireless communication technologies. It is further possible that signals of Meters are amplified by other devices or other Meters on the physical level without violating this assumption. However, it is assumed that the Meters do only communicate with the TOE and that only the TOE is able to decrypt the data sent by the Meter.

It is essential that Processing Profiles correctly define the amount of information that must be sent to an external entity. Exact regulations regarding the Processing Profiles and the Gateway Administrator are beyond the scope of this Security Target.

3.4 Threats

The following sections identify the threats that are posed against the assets handled by the Smart Meter System. Those threats are the result of a threat model that has been developed for the whole Smart Metering System first and then has been focussed on the threats against the Gateway. It should be noted that the threats in the following paragraphs consider two different kinds of attackers:

- Attackers having physical access to Meter, Gateway, a connection between these components or local logical access to any of the interfaces (local attacker), trying to disclose or alter assets while stored in the Gateway or while transmitted between Meters in the LMN and the Gateway. Please note that the following threat model assumes that the local attacker has less motivation than the WAN attacker as a successful attack of a local attacker will always only impact one Gateway. Please further note that the local attacker includes authorised individuals like consumers.
- An attacker located in the WAN (WAN attacker) trying to compromise the confidentiality and/or integrity of the processed Meter Data and or configuration data transmitted via the WAN, or attacker trying to conquer a component of the infrastructure (i.e. Meter, Gateway or Controllable Local System) 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 entity).

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

T.DataModificationLocal A local attacker may try to modify (i.e. alter, delete, insert, replay or redirect) Meter Data when transmitted between Meter and Gateway, Gateway and Consumer, or Gateway and external entities. The objective of the attacker may be to alter billing-relevant information or grid status information. The attacker may perform the attack via any interface (LMN, HAN, or WAN).

In order to achieve the modification, the attacker may also try to modify secondary assets like the firmware or configuration parameters of the Gateway.

T.DataModificationWAN A WAN attacker may try to modify (i.e. alter, delete, insert, replay or redirect) Meter Data, Gateway config data, Meter config data, CLS config data or a firmware update when transmitted between the Gateway and an external entity in the WAN.

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

When trying to modify config data or a firmware update, the WAN attacker tries to circumvent security mechanisms of the TOE or tries to get control over the TOE or a device in the LAN that is protected by the TOE.

T.TimeModification A local attacker or WAN attacker may try to alter the Gateway time. The motivation of the attacker could be e.g. 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 WAN attacker may try to violate the privacy of the Consumer by disclosing Meter Data or configuration data (Meter config, Gateway config or CLS config) or parts of it when transmitted between Gateway and external entities in the WAN.

T.DisclosureLocal A local attacker may try to violate the privacy of the Consumer by disclosing Meter Data transmitted between the TOE and the Meter. This threat is of specific importance if Meters of more than one Consumer are served by one Gateway.

T.Infrastructure A WAN attacker may try to obtain control over Gateways, Meters or CLS via the TOE, which enables the WAN attacker to cause damage to Consumers or external entities or the grids used for commodity distribution (e.g. by sending wrong data to an external entity).

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

T.ResidualData By physical and/or logical means a local attacker or a WAN attacker may try to read out data from the Gateway, which travelled through the Gateway before and which are no longer needed by the Gateway (i.e. Meter Data, Meter config, or CLS config).

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

While the WAN attacker only uses the logical interface of the TOE that is provided into the WAN, the local attacker may also physically access the TOE.

T.Privacy A WAN attacker may try to obtain more detailed information from the Gateway than actually required to fulfil the tasks defined by its role or the contract with the Consumer. This includes scenarios in which an external entity that is primarily authorised to obtain information from the TOE tries to obtain more information than the information that has been authorised as well as scenarios in which an attacker who is not authorised at all tries to obtain information.

3.5 Organizational Security Policies

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

OSP.SM The TOE shall use the services of a certified Security Module for

- verification of digital signatures,
- generation of digital signatures,
- key agreement,
- key transport,
- key storage,
- Random Number Generation,

The Security Module shall be certified according to [SecModPP] and shall be used in accordance with its relevant guidance documentation.

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

1. A system log of relevant events in order to allow an authorised Gateway Administrator to analyse the status of the TOE. The TOE shall also analyse 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 chapter 6.2.1) that provides the Gateway Administrator 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 authorised Gateway

Administrator via the IF_GW_WAN interface of the TOE and an authorised Service Technician via the IF_GW_SRV interface of the TOE.

2. Access to the information in the calibration log shall only be allowed for an authorised Gateway Administrator via the IF_GW_WAN interface of the TOE.
3. Access to the information in the consumer log shall only be allowed for an authorised Consumer via the IF_GW_CON interface of the TOE. 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 amount of events is available (in order to allow a Consumer to verify an invoice) but may overwrite older events in case that the audit trail gets full.

For the calibration log, however, the TOE shall ensure the availability of all events over the lifetime of the TOE.

4 Security Objectives

4.1 Security Objectives for the TOE

O.Firewall The TOE shall serve as the connection point for the connected devices within the LAN 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 Gateway) and itself against threats from the WAN side.

The firewall:

- shall allow only connections established from HAN or the TOE itself to the WAN (i.e. from devices in the HAN to external entities in the WAN or from the TOE itself to external entities in the WAN),
- shall provide a wake-up service on the WAN side interface,
- shall not allow connections from the LMN to the WAN,
- shall not allow any other services being offered on the WAN side interface,
- shall not allow connections from the WAN to the LAN or to the TOE itself,
- shall enforce communication flows by allowing traffic from CLS in the HAN to the WAN only if confidentiality-protected and integrity-protected and if endpoints are authenticated.

O.SeparateIF The TOE shall have physically separated ports for the LMN, the HAN and the WAN and shall automatically detect during its self test whether connections (wired or wireless), if any, are wrongly connected.

Application Note 3: O.SeparateIF refers to physical interfaces and must not be fulfilled by a pure logical separation of one physical interface only.

O.Conceal 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 analysing the frequency, load, size or the absence of external communication.[24]

O.Meter The TOE receives or polls information about the consumption or production of different commodities from one or multiple Meters and is responsible for handling this Meter Data.

This includes that:

- The TOE shall ensure that the communication to the Meter(s) is established in an Gateway Administrator-definable interval or an interval as defined by the Meter,
- the TOE shall enforce encryption and integrity protection for the communication with the Meter[25],
- the TOE shall verify the integrity and authenticity of the data received from a Meter before handling it further,
- the TOE shall process the data according to the definition in the corresponding Processing Profile,
- the TOE shall encrypt the processed Meter Data for the final recipient, sign the data and
- deliver the encrypted data to authorised external entities as defined in the corresponding Processing Profiles facilitating an encrypted channel,
- the TOE shall store processed Meter Data if an external entity cannot be reached and re-try to send

[24] It should be noted that this requirement only applies to communication flows in the WAN.

[25] It is acknowledged that the implementation of a secure channel between the Meter and the Gateway is a security function of both units. The TOE as defined in this Security Target only has a limited possibility to secure this communication as both sides have to sign responsible for the quality of a cryptographic connection. However, it should be noted that the encryption of this channel only needs to protect against the Local Attacker possessing a basic attack potential and that the Meter utilises the services of its Security Module to negotiate the channel.

the data until a configurable number of unsuccessful retries has been reached,

- 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.

O.Crypt

The TOE shall provide cryptographic functionality as follows:

- authentication, integrity protection and encryption of the communication and data to external entities in the WAN,
- authentication, integrity protection and encryption of the communication to the Meter,
- authentication, integrity protection and encryption of the communication to the Consumer,
- replay detection for all communications with external entities,
- encryption of the persistently stored TSF and user data of the TOE[26].

In addition, the TOE shall generate the required keys utilising the services of its Security Module[27], ensure that the keys are only used for an acceptable amount of time and destroy ephemeral[28] keys if no longer needed.[29]

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.

[26] The encryption of the persistent memory shall support the protection of the TOE against local attacks.

[27] Please refer to chapter 1.4.7 for an overview on how the cryptographic functions are distributed between the TOE and its Security Module.

[28] This objective addresses the destruction of ephemeral keys only because all keys that need to be stored persistently are stored in the Security Module.

[29] Please refer to chapter F.9 of part 2 of [CC] for more detailed information about what kind of information this objective applies to.

O.Protect

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

Specifically, the TOE shall

- encrypt its TSF and user data as long as it is not in use,
- overwrite any information that is no longer needed to ensure that it is no longer available via the external interfaces of the TOE[30],
- monitor user data and the TOE firmware for integrity errors,
- contain a test that detects whether the interfaces for WAN and LAN are separate,
- have a fail-safe design that specifically ensures that no malfunction can impact the delivery of a commodity (e.g. energy, gas, heat or water)[31],
- make any physical manipulation within the scope of the intended environment detectable for the Consumer and Gateway Administrator.

O.Management

The TOE shall only provide authorised Gateway Administrators with functions for the management of the security features.

The TOE shall ensure that any change in the behaviour of the security functions can only be achieved from the WAN side interface. Any management activity from a local interface may only be read only.

Further, the TOE shall implement a secure mechanism to update the firmware of the TOE that ensures that only authorised entities are able to provide updates for the TOE

[30] Please refer to chapter F.9 of part 2 of [CC] for more detailed information about what kind of information this objective applies to.

[31] Indeed this Security Target acknowledges that the Gateway and the Meters have no possibility at all to impact the delivery of a commodity. Even an intentional stop of the delivery of a certain commodity is not within the scope of this Security Target. It should however be noted that such a functionality may be realised by a CLS that utilises the services of the TOE for its communication.

and that only authentic and integrity protected updates are applied.

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

1. A system log of relevant events in order to allow an authorised Gateway Administrator or an authorised Service Technician to analyse the status of the TOE. The TOE shall also analyse 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 and information about the system status (including relevant error messages).
3. A calibration log that provides the Gateway Administrator 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 authorised Gateway Administrator via IF_GW_WAN or for an authorised Service Technician via IF_GW_SRV.
2. Access to the information in the consumer log shall only be allowed for an authorised Consumer via the IF_GW_CON 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. Read-only access to the information in the calibration log shall only be allowed for an authorised

Gateway Administrator via the WAN 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 amount of events is available (in order to allow a Consumer to verify an invoice) but may overwrite older events in case that the audit trail gets full.

For the calibration log however, the TOE shall ensure the availability of all events over the lifetime of the TOE.

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[32]. Access control shall depend on the destination interface that is used to send that information.

4.2 Security Objectives for the Operational Environment

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

OE.TrustedAdmins The Gateway Administrator and the Service Technician shall be trustworthy and well-trained.

OE.PhysicalProtection The TOE shall be installed in a non-public environment within the premises of the Consumer that provides a basic level of physical protection. This protection shall cover the TOE, the Meters that the TOE communicates with and the communication channel between the TOE and its Security

[32] While in classical access control mechanisms the Gateway Administrator gets complete access, the TOE also maintains a set of information (specifically the consumer log) to which Gateway Administrators have restricted access.

Module. Only authorised individuals may physically access the TOE.

OE.Profile The Processing 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

- verification of digital signatures,
- generation of digital signatures,
- key agreement,
- key transport,
- key storage,
- Random Number Generation.

The Security Module used shall be certified according to [SecModPP] and shall be used in accordance with its relevant guidance documentation.

OE.Update The firmware updates for the Gateway that can be provided by an authorised external entity shall undergo a certification process according to this Security Target before they are issued to show that the update is implemented correctly. The external entity that is authorised 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

- a WAN network connection with a sufficient reliability and bandwidth for the individual situation is available,
- one or more trustworthy sources for an update of the system time are available in the WAN,
- the Gateway is the only communication gateway for Meters in the LMN,

- if devices in the HAN have a separate connection to parties in the WAN (beside the Gateway) this connection is appropriately protected.

OE.Keygen It shall be ensured that the ECC key pair for a Meter (TLS) is generated securely according to the [TR-03109-3]. It shall also be ensured that the keys are brought into the Gateway in a secure way by the Gateway Administrator.

4.3 Security Objective Rationale

4.3.1 Overview

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

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Management	O.Log	O.Access	OE.SM	OE.ExternalPrivacy	OE.TrustedAdmins	OE.PhysicalProtec-	OE.Profile	OE.Update	OE.Network	OE.Keygen
T.DataModification-Local				X	X		X	X					X	X				
T.DataModification-WAN	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			
OSP.SM					X		X	X			X		X					
OSP.Log							X	X	X	X			X					
A.ExternalPrivacy	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨		X						
A.TrustedAdmins	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨			X					
A.PhysicalProtection	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨				X				
A.ProcessProfile	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨					X			
A.Update	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨						X		
A.Network	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨							X	
A.Keygen	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨								X

Table 8: 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 Gateway Administrator and Service Technician. **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**, **O.Log** 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 objectives together ensure that the communication between the Meter and the TOE 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 LAN 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 Gateway) 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 WAN 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 in the WAN. 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.Conceal** and **O.Crypt**.

O.Firewall defines the connections for the devices within the LAN 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 Gateway) 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.Conceal 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. Both objectives together ensure that the communication between the Meter and the TOE 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 Gateway Administrator (**OE.TrustedAdmins**) who could realise a physical manipulation contribute to counter this threat.

The aspect of a WAN attacker is covered by **O.Firewall** as this objective ensures that an adequate level of protection is realised 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 parties 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.

Finally, **O.Conceal** 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 organisational 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 utilises 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 utilised 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 Gateway Administrators 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**.

4.3.4 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.ProcessProfile

The assumption **A.ProcessProfile** 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.

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.

5.2 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.

5.3 Component levelling

FPR_CON: Communication concealing ------------1

5.4 Management

The following actions could be considered for the management functions in FMT:

a. Definition of the interval in FPR_CON.1.2 if definable within the operational phase of the TOE.

5.5 Audit

There are no auditable events foreseen.

5.6 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: *weekly, daily, hourly, [assignment: other interval]*] to conceal the data flow.**

6 Security Requirements

6.1 Overview

This chapter describes the security functional and the assurance requirements which have to be fulfilled by the TOE. Those requirements comprise functional components from part 2 of [CC] and the assurance components as defined for the Evaluation Assurance Level 4 from part 3 of [CC].

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] in stating a requirement.
- **Assignment** operation (denoted by *italicised 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. FDP_IFC.2/FW).

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

The following table summarises all TOE security functional requirements of this ST:

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.4/SYS	Prevention of audit data loss for the system log
FAU_GEN.1/CON	Audit data generation for consumer log

FAU_SAR.1/CON	Audit review for consumer log
FAU_STG.4/CON	Prevention of audit data loss for the consumer log
FAU_GEN.1/CAL	Audit data generation for calibration log
FAU_SAR.1/CAL	Audit review for calibration log
FAU_STG.4/CAL	Prevention of audit data loss for the calibration log
FAU_GEN.2	User identity association
FAU_STG.2	Guarantees of audit data availability
Class FCO: Communication	
FCO_NRO.2	Enforced proof of origin
Class FCS: Cryptographic Support	
FCS_CKM.1/TLS	Cryptographic key generation for TLS
FCS_COP.1/TLS	Cryptographic operation for TLS
FCS_CKM.1/CMS	Cryptographic key generation for CMS
FCS_COP.1/CMS	Cryptographic operation for CMS
FCS_CKM.1/MTR	Cryptographic key generation for Meter communication encryption
FCS_COP.1/MTR	Cryptographic operation for Meter communication encryption
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1/HASH	Cryptographic operation for Signatures
FCS_COP.1/MEM	Cryptographic operation for TSF and user data encryption

Class FDP: User Data Protection	
FDP_ACC.2	Complete Access Control
FDP_ACF.1	Security attribute based access control
FDP_IFC.2/FW	Complete information flow control for firewall
FDP_IFF.1/FW	Simple security attributes for Firewall
FDP_IFC.2/MTR	Complete information flow control for Meter information flow
FDP_IFF.1/MTR	Simple security attributes for Meter information
FDP_RIP.2	Full residual information protection
FDP_SDI.2	Stored data integrity monitoring and action
Class FIA: Identification and Authentication	
FIA_ATD.1	User attribute definition
FIA_AFL.1	Authentication failure handling
FIA_UAU.2	User authentication before any action
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU.6	Re-Authenticating
FIA_UID.2	User identification before any action
FIA_USB.1	User-subject binding
Class FMT: Security Management	
FMT_MOF.1	Management of security functions behaviour
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles

FMT_MSA.1/AC	Management of security attributes for Gateway access policy
FMT_MSA.3/AC	Static attribute initialisation for Gateway access policy
FMT_MSA.1/FW	Management of security attributes for Firewall policy
FMT_MSA.3/FW	Static attribute initialisation for Firewall policy
FMT_MSA.1/MTR	Management of security attributes for Meter policy
FMT_MSA.3/MTR	Static attribute initialisation for Meter policy
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_RPL.1	Replay Detection
FPT_STM.1	Reliable time stamps
FPT_TST.1	TSF testing
FPT_PHP.1	Passive detection of physical attack
Class FTP: Trusted path/channels	
FTP_ITC.1/WAN	Inter-TSF trusted channel for WAN
FTP_ITC.1/MTR	Inter-TSF trusted channel for Meter
FTP_ITC.1/USR	Inter-TSF trusted channel for User

Table 9: List of Security Functional Requirements

6.2 Class FAU: Security Audit

6.2.1 Introduction

The TOE compliant to this Security Target shall implement three different audit logs as defined in **OSP.Log** and **O.Log**. The following table provides an overview over the three audit logs before the following chapters introduce the SFRs related to those audit logs.

	System-Log	Consumer-Log	Calibration-Log
Purpose	● Inform the Gateway Administrator about security relevant events ● Log all events as defined by Common Criteria [CC] for the used SFR • Log all system relevant events on specific functionality • Automated alarms in case of a cumulation of certain events • Inform the Service Technician about the status of the Gateway	• Inform the Consumer about all information flows to the WAN • Inform the Consumer about the Processing Profiles • Inform the Consumer about other metering data (not billing-relevant) • Inform the Consumer about all billing-relevant data needed to verify an invoice	• Track changes that are relevant for the calibration of the TOE relevant data needed to verify an invoice
Data	• As defined by CC part 2 • Augmented by specific events for the security functions	• Information about all information flows to the WAN • Information about the current and the previous Processing Profiles • Non-billing-relevant Meter Data • Information about the system status (including relevant errors)	• Calibration relevant data only

		• Billing-relevant data needed to verify an invoice	
Access	• Access by authorised Gateway Administrator and via IF_GW_WAN only • Events may only be deleted by an authorised Gateway Administrator via IF_GW_WAN • Read access by authorised Service Technician via IF_GW_SRV only	• Read access by authorised Consumer and via IF_GW_CON only to the data related to the current consumer	• Read access by authorised Gateway Administrator and via IF_GW_WAN only
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 • Retention period is set by authorised Gateway Administrator on request by consumer, data older than this are deleted.	• The availability of data has to be ensured over the lifetime of the TOE.

Table 10: Overview over audit processes

6.2.2 Security Requirements for the System Log

6.2.2.1 Security audit automatic response (FAU_ARP)

6.2.2.1.1 FAU_ARP.1/SYS: Security Alarms for system log

FAU_ARP.1.1/SYS The TSF shall ~~take~~ *inform an authorised Gateway Administrator and create a log entry in the system log* [33] upon detection of a potential security violation.

Hierarchical to: No other components

Dependencies: FAU_SAA.1 Potential violation analysis

6.2.2.2 Security audit data generation (FAU_GEN)

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

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

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

b) All auditable events for the basic[34] level of audit; and

c) *other non privacy relevant auditable events: none*[35].

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the **~~PP/~~ST**[36], *other audit relevant information: none* [37].

[33] [assignment: *list of actions*]

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

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

[36] [refinement: *PP/ST*]

[37] [assignment*: other audit relevant information*]

Hierarchical to: No other components

Dependencies: FPT_STM.1

6.2.2.3 Security audit analysis (FAU_SAA)

6.2.2.3.1 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

- *Start-up and shutdown of the audit functions*
- *all auditable events for the basic level of audit*
- *all types of failures in the TSF as listed in FPT_FLS.1* [38]

known to indicate a potential security violation.

b) *any other rules: none* [39].

Hierarchical to: No other components

Dependencies: FAU_GEN.1

6.2.2.4 Security audit review (FAU_SAR)

6.2.2.4.1 FAU_SAR.1/SYS: Audit Review for system log

FAU_SAR.1.1/SYS The TSF shall provide *only authorised Gateway Administrators via the IF_GW_WAN interface and authorised Service Technicians via the IF_GW_SRV*

[38] [assignment: *subset of defined auditable events*]

[39] [assignment: *any other rules*]

interface [40] with the capability to read all information [41] from the **system** audit records [42].

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

Hierarchical to: No other components

Dependencies: FAU_GEN.1

6.2.2.5 Security audit event storage (FAU_STG)

6.2.2.5.1 FAU_STG.4/SYS: Prevention of audit data loss for systemlog

FAU_STG.4.1/SYS The TSF shall overwrite the oldest stored audit records [43] and other actions to be taken in case of audit storage failure: none [44] if the **system** audit trail [45] is full.

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

Application Note 4: The size of the audit trail that is available before the oldest events get overwritten is configurable for the Gateway Administrator.

[40] [assignment: *authorised users*]

[41] [assignment: *list of audit information*]

[42] [refinement: *audit records*]

[43] [selection, choose one of: "*ignore audited events*", "*prevent audited events, except those taken by the authorised user with special rights*", "*overwrite the oldest stored audit records*"]

[44] [assignment: *other actions to be taken in case of audit storage failure*]

[45] [refinement: *audit trail*]

6.2.3 Security Requirements for the Consumer Log

6.2.3.1 Security audit data generation (FAU_GEN)

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

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

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

b) All auditable events for the not specified[46] level of audit; and

c) *all audit events as listed in Table 11 and additional events: none* [47].

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the **~~PP/~~ST**[48], *additional information as listed in Table 11 and additional events: none* [49].

Hierarchical to: No other components

Dependencies: FPT_STM.1

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

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

[48] [refinement: *PP/ST*]

[49] [assignment*: other audit relevant information*]

Event	Additional Information
Any change to a Processing Profile	The new and the old Processing Profile
Any submission of Meter Data to an external entity	The Processing Profile that lead to the submission The submitted values
Any submission of Meter Data that is not billing-relevant	-
Billing-relevant data	-
Any administrative action performed	-
Relevant system status information including relevant errors	-

Table 11: Events for consumer log

6.2.3.2 Security audit review (FAU_SAR)

6.2.3.2.1 FAU_SAR.1/CON: Audit Review for consumer log

FAU_SAR.1.1/CON The TSF shall provide *only authorised Consumer via the IF_GW_CON interface*[50] with the capability to read *all*

[50] [assignment: *authorised users*]

information that are related to them [51] from the **consumer** audit records [52].

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

Hierarchical to: No other components

Dependencies: FAU_GEN.1

Application Note 5: 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 Security audit event storage (FAU_STG)

6.2.3.3.1 FAU_STG.4/CON: Prevention of audit data loss for the consumer log

FAU_STG.4.1/CON The TSF shall overwrite the oldest stored audit records and *interrupt metrological operation in case that the oldest audit record must still be kept for billing verification* [53] if the **consumer** audit trail is full.

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

Application Note 6: The size of the audit trail that is available before the oldest events get overwritten is configurable for the Gateway Administrator.

[51] [assignment: *list of audit information*]

[52] [refinement: *audit records*]

[53] [assignment: *other actions to be taken in case of audit storage failure*]

6.2.4 Security Requirements for the Calibration Log

6.2.4.1 Security audit data generation (FAU_GEN)

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

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

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

b) All auditable events for the not specified [54] level of audit; and

c) *all calibration-relevant information according to Table 12*[55].

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the **~~PP~~/ST** [56], *other audit relevant information: none* [57].

Hierarchical to: No other components

Dependencies: FPT_STM.1

Application Note 7: The calibration log serves to fulfil national requirements in the context of the calibration of the TOE.

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

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

[56] [refinement: *PP/ST*]

[57] [assignment: *other audit relevant information*]

Event / Parameter	**Content**
Commissioning	Commissioning of the SMGW MUST be logged in calibration log.
Event of self-test	Initiation of self-test MUST be logged in calibration log.
New meter	Connection and registration of a new meter MUST be logged in calibration log.
Meter removal	Removal of a meter from SMGW MUST be logged in calibration log.
Change of tarification profiles	Every change (incl. parameter change) of a tarification profile according to [**TR-03109-1**, 4.4], provided the parameter is relevant for calibration regulations (see below) as well as new storage or removal of tarification profiles MUST be logged in calibration log. Parameter relevant for calibration regulations are: • Device-ID of a meter - Unique identifier of the meter, which send the input values for a TAF • OBIS value of the measured variable of the meter - Unique value for the measured variable of the meter for the used TAF • Metering point name - Unique name of the metering point • Billing period - Period in which a billing should be done • Consumer ID • Validity period - Period for which the TAF is booked • Definition of tariff stages - Defines different tariff stages and associated OBIS values. Here it will be defined which tariff stage is valid at the time of rule set activation • Tariff switching time - Defines to the split second the switching of tariff stages. The time points can be defined as periodic values • Register period - Time distance of two consecutive measured value acquisitions for meter readings

Change of meter profiles	Every change (incl. parameter change) of a meter profile according to [**TR-03109-1**, 4.4], provided the parameter is relevant for calibration regulations (see below) as well as new storage or removal of meter profiles MUST be logged in calibration log. Parameter relevant for legal metrology are: • Device-ID - Unique identifier of the meter according to **DIN 43863-5** • Key material - Public key for inner signature (dependent on the used meter in LMN) • Register period - Interval during receipt of meter values • Displaying interval (‘Anzeigeintervall’) - Interval during which the actual meter value (only during display) must be updated in case of bidirectional communication between meter and SMGW • Balancing (‘Saldierend’) - Determines if the meter is balancing (‘saldierend’) and meter values can grow and fall • OBIS values - OBIS values according to **IEC-62056-6-1** resp. EN 13757-1 • Converter factor (‘Wandlerfaktor’) - Value is 1 in case of directly connected meter. In usage of converter counter (‘Wandlerzähler’) the value may be different.
Software update	Every update of the code which touches calibration regulations (serialized COSEM-objects, rules) MUST be logged in calibration log.
Firmware update	Every firmware update (incl. operating system update if applicable) MUST be logged in calibration log.
Error messages of a meter	All FATAL messages of a connected meter MUST be logged in calibration log according to 0 - no error 1 - Warning, no action to be done according to calibration authority, meter value valid

	2 - Temporal error, send meter value will be marked as invalid, the value in meter field (‘Messwertfeld’) could be used according to the rules of [**VDE4400**] resp. [**G865**] as replacement value (‘Ersatzwert’) in backend. 3 - Temporal error, send meter value is invalid; the value in the meter field (‘Messwertfeld’) cannot be used as replacement value in backend. 4 - Fatal error (meter defect), actual send value is invalid and all future values will be invalid. including the device-ID.
Error messages of a SMGW	All self-test and calibration regulations relevant errors MUST be logged in calibration log.

1506 **Table 12: Content of calibration log**

1507

6.2.4.2 Security audit review (FAU_SAR)

6.2.4.2.1 FAU_SAR.1/CAL: Audit Review for the calibration log

FAU_SAR.1.1/CAL The TSF shall provide *only authorised Gateway Administrators via the IF_GW_WAN interface* [58] with the capability to read *all information* [59] from the **calibration** audit records [60].

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

Hierarchical to: No other components

Dependencies: FAU_GEN.1

6.2.4.3 Security audit event storage (FAU_STG)

6.2.4.3.1 FAU_STG.4/CAL: Prevention of audit data loss for calibration log

FAU_STG.4.1/CAL The TSF shall ignore audited events [61] and *stop the operation of the TOE and inform a Gateway Administrator* [62] if the **calibration** audit trail [63] is full.

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

Application Note 8: As outlined in the introduction it has to be ensured that the events of the calibration log are available over the lifetime of the TOE.

[58] [assignment: *authorised users*]

[59] [assignment: *list of audit information*]

[60] [refinement: *audit records*]

[61] [selection, choose one of: "*ignore audited events*", "*prevent audited events, except those taken by the authorised user with special rights*", "*overwrite the oldest stored audit records*"]

[62] [assignment: *other actions to be taken in case of audit storage failure*]

[63] [refinement: *audit trail*]

6.2.5 Security Requirements that apply to 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
	FIA_UID.1
Application Note 9:	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.2: Guarantees of audit data availability

FAU_STG.2.1 The TSF shall protect the stored audit records in ~~**the**~~ **all** audit trail**s** [64] from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to prevent [65] unauthorised modifications to the stored audit records in ~~**the**~~ **all** audit trail**s** [66].

FAU_STG.2.3 The TSF shall ensure that *all* [67] stored audit records will be maintained when the following conditions occur: audit storage exhaustion or failure [68].

Hierarchical to: FAU_STG.1 Protected audit trail storage

Dependencies: FAU_GEN.1

Application Note 10: Please note that FAU_STG.2 applies to all audit logs, the system log, the calibration log, and the consumer log.

[64] [refinement: *audit trail*]

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

[66] [refinement: *audit trail*]

[67] [assignment: *metric for saving audit records*]

[68] [selection: *audit storage exhaustion, failure, attack*]

6.3 Class FCO: Communication

6.3.1 Non-repudiation of origin (FCO_NRO)

6.3.1.1 FCO_NRO.2: Enforced proof of origin

FCO_NRO.2.1 The TSF shall enforce the generation of evidence of origin for transmitted *Meter Data* [69] at all times.

FCO_NRO.2.2 The TSF shall be able to relate the *key material used for signature* [70, 71] of the originator of the information, and the *signature* [72] of the information to which the evidence applies.

FCO_NRO.2.3 The TSF shall provide a capability to verify the evidence of origin of information to *recipient, Consumer* [73] given *limitations of the digital signature according to TR-03109-1* [74].

Hierarchical to: FCO_NRO.1 Selective proof of origin

Dependencies: FIA_UID.1 Timing of identification

Application Note 11: FCO_NRO.2 requires that the TOE calculates a signature over Meter Data that is submitted to external entities.

Therefore, the TOE has to create a hash value over the Data To Be Signed (DTBS) as defined in FCS_COP.1/HASH. The creation of the actual signature however is performed by the Security Module.

[69] [assignment: *list of information types*]

[70] [assignment: *list of attributes*]

[71] The key material here also represents the identity of the Gateway.

[72] [assignment: *list of information fields*]

[73] [selection: *originator, recipient, [assignment: list of third parties]*]

[74] [assignment: *limitations on the evidence of origin*]

6.4 Class FCS: Cryptographic Support

6.4.1 Cryptographic support for TLS

6.4.1.1 Cryptographic key management (FCS_CKM)

6.4.1.1.1 FCS_CKM.1/TLS: Cryptographic key generation for TLS

FCS_CKM.1.1/TLS: The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *TLS-PRF with SHA-256 or SHA-384* [75] and specified cryptographic key sizes *128 bit, 256 bit or 384 bit* [76] that meet the following: *[RFC 5246] in combination with [FIPS Pub. 180-4] and [RFC 2104]* [77].

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation], fulfilled by FCS_COP .1/TLS

FCS_CKM.4 Cryptographic key destruction

Application Note 12: The Security Module is used for the generation of random numbers and for all cryptographic operations with the private key of a TLS certificate.

Application Note 13: The TOE uses only cryptographic specifications and algorithms as described in [TR-03109-3].

6.4.1.2 Cryptographic operation (FCS_COP)

6.4.1.2.1 FCS_COP.1/TLS: Cryptographic operation for TLS

FCS_COP.1.1/TLS: The TSF shall perform *TLS encryption, decryption, and integrity protection* [78] in accordance with a specified cryptographic algorithm *TLS cipher suites*

[75] [assignment: *key generation algorithm*]

[76] [assignment: *cryptographic key sizes*]

[77] [assignment: *list of standards*]

[78] [assignment: *list of cryptographic operations*]

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, and TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 [79] *using elliptic curves BrainpoolP256r1, BrainpoolP384r1, BrainpoolP512r1 (according to [RFC 5639]), NIST P-256, and NIST P-384 (according to [RFC 5114])* and cryptographic key sizes *128 bit or 256 bit* [80] that meet the following: *[RFC 2104], [RFC 5114], [RFC 5246], [RFC 5289], [RFC 5639], [NIST 800-38A], and [NIST 800-38D]* [81].

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation], fulfilled by

FCS_CKM.1/TLS

FCS_CKM.4 Cryptographic key destruction

Application Note 14: The TOE uses only cryptographic specifications and algorithms as described in [TR-03109-3].

6.4.2 Cryptographic support for CMS

6.4.2.1 Cryptographic key management (FCS_CKM)

6.4.2.1.1 FCS_CKM.1/CMS: Cryptographic key generation for CMS

FCS_CKM.1.1/CMS The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECKA-EG* [82] and specified cryptographic key sizes *128*

[79] [assignment: *cryptographic algorithm*]

[80] [assignment: *cryptographic key sizes*]

[81] [assignment: *list of standards*]

[82] [assignment: *cryptographic key generation algorithm*]

bit[83] that meet the following: *[X9.63] in combination with [RFC 3565]*[84].

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation], fulfilled by FCS_COP.1/CMS

FCS_CKM.4 Cryptographic key destruction

Application Note 15: The TOE utilises the services of its Security Module for the generation of random numbers and for all cryptographic operations with the private asymmetric key of a CMS certificate.

Application Note 16: The TOE uses only cryptographic specifications and algorithms as described in [TR-03109-3].

6.4.2.2 Cryptographic operation (FCS_COP)

6.4.2.2.1 FCS_COP.1/CMS: Cryptographic operation for CMS

FCS_COP.1.1/CMS The TSF shall perform *symmetric encryption, decryption and integrity protection* in accordance with a specified cryptographic algorithm *AES-CBC-CMAC or AES-GCM*[85] and cryptographic key sizes *128 bit*[86] that meet the following: *[FIPS Pub. 197],*

[83] [assignment: *cryptographic key sizes*]

[84] [assignment: *list of standards*]

[85] [assignment*: list of cryptographic operations*]

[86] [assignment: *cryptographic key sizes*]

*[NIST 800-38D], [*RFC 4493*], [RFC 5084], and [RFC 5652] in combination with [NIST 800-38A]* [87]*.*

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation], fulfilled by

FCS_CKM.1/CMS

FCS_CKM.4 Cryptographic key destruction

Application Note 17: The TOE uses only cryptographic specifications and algorithms as described in [TR-03109-3].

6.4.3 Cryptographic support for Meter communication encryption

6.4.3.1 Cryptographic key management (FCS_CKM)

6.4.3.1.1 FCS_CKM.1/MTR: Cryptographic key generation for Meter communication (symmetric encryption)

FCS_CKM.1.1/MTR The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *AES-CMAC* [88] and specified cryptographic key sizes *128 bit* [89] that meet the following: *[FIPS Pub. 197], and [RFC 4493]* [90].

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation], fulfilled by FCS_COP.1/MTR

FCS_CKM.4 Cryptographic key destruction

[87] [assignment: *list of standards*]

[88] [assignment: *cryptographic key generation algorithm*]

[89] [assignment: *cryptographic key sizes*]

[90] [assignment: *list of standards*]

Application Note 18: The TOE uses only cryptographic specifications and algorithms as described in [TR-03109-3].

6.4.3.2 Cryptographic operation (FCS_COP)

6.4.3.2.1 FCS_COP.1/MTR: Cryptographic operation for Meter communication encryption

FCS_COP.1.1/MTR The TSF shall perform symmetric encryption, decryption, integrity protection[91] in accordance with a specified cryptographic algorithm AES-CBC-CMAC[92] and cryptographic key sizes 128 bit[93] that meet the following: [FIPS Pub. 197] and [RFC 4493] in combination with [ISO 10116][94].

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation], fulfilled by

FCS_CKM.1/MTR

FCS_CKM.4 Cryptographic key destruction

Application Note 19: The ST allows different scenarios of key generation for Meter communication encryption. Those are:

1. If a TLS encryption is being used, the key generation/negotiation is as defined by FCS_CKM.1/TLS.
2. If AES encryption is being used, the key has been brought into the Gateway via a management function during the pairing process for the Meter

[91] [assignment*: list of cryptographic operations*]

[92] [assignment*: cryptographic algorithm*]

[93] [assignment*: cryptographic key sizes*]

[94] [assignment: *list of standards*]

(see FMT_SMF.1) as defined by FCS_COP.1/MTR.

Application Note 20: If the connection between the Meter and TOE is unidirectional, the communication between the Meter and the TOE is secured by the use of a symmetric AES encryption. If a bidirectional connection between the Meter and the TOE is established, the communication is secured by a TLS channel as described in chapter 6.4.1. As the TOE shall be interoperable with all kind of Meters, both kinds of encryption are implemented.

Application Note 21: The TOE uses only cryptographic specifications and algorithms as described in [TR-03109-3].

6.4.4 General Cryptographic support

6.4.4.1 Cryptographic key management (FCS_CKM)

6.4.4.1.1 FCS_CKM.4: Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *Zeroisation* [95] that meets the following: *none* [96].

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation], fulfilled by FCS_CKM.1/TLS and

FCS_CKM.1/CMS and FCS_CKM.1/MTR

Application Note 22: Please note that as against the requirement FDP_RIP.2, the mechanisms implementing the requirement from FCS_CKM.4 shall be suitable to avoid attackers with

[95] [assignment: *cryptographic key destruction method*]

[96] [assignment: *list of standards*]

physical access to the TOE from accessing the keys after they are no longer used.

6.4.4.2 Cryptographic operation (FCS_COP)

6.4.4.2.1 *FCS_COP.1/HASH: Cryptographic operation, hashing for signatures*

FCS_COP.1.1/HASH — The TSF shall perform *hashing for signature creation and verification* [97] in accordance with a specified cryptographic algorithm *SHA-256, SHA-384 and SHA-512* [98] and cryptographic key sizes *none* [99] that meet the following: *[FIPS Pub. 180-4]*[100].

Hierarchical to: — No other components.

Dependencies: — [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation [101]]

FCS_CKM.4 Cryptographic key destruction

Application Note 23: — 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 24: — The TOE uses only cryptographic specifications and algorithms as described in [TR-03109-3].

[97] [assignment*: list of cryptographic operations*]

[98] [assignment: *cryptographic algorithm*]

[99] [assignment: *cryptographic key sizes*]

[100] [assignment: *list of standards*]

[101] The justification for the missing dependency FCS_CKM.1 can be found in chapter 6.12.1.3.

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

FCS_COP.1.1/MEM The TSF shall perform *TSF and user data encryption and decryption* [102] in accordance with a specified cryptographic algorithm *AES-XTS* [103] and cryptographic key sizes *128 bit* [104] that meet the following: *[FIPS Pub. 197] and [NIST 800-38E]* [105].

Hierarchical to: No other components.

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation], not fulfilled s. Application Note 25

FCS_CKM.4 Cryptographic key destruction

Application Note 25: Please note that for the key generation process an external security module is used during TOE production.

Application Note 26: The TOE encrypts its local TSF and user data while it is not in use (i.e. while stored in a persistent memory).

It shall be noted that this kind of encryption cannot provide an absolute protection against physical manipulation and does not aim to. It however contributes to the security concept that considers the protection that is provided by the environment.

[102] [assignment*: list of cryptographic operations*]

[103] [assignment*: cryptographic algorithm*]

[104] [assignment*: cryptographic key sizes*]

[105] [assignment: *list of standards*]

6.5 Class FDP: User Data Protection

6.5.1 Introduction to the Security Functional Policies

The security functional requirements that are used in the following chapters implicitly define a set of Security Functional Policies (SFP). These policies are introduced in the following paragraphs in more detail to facilitate the understanding of the SFRs:

- The **Gateway 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 [TR-03109-1].
- The **Firewall SFP** implements an information flow policy to fulfil the objective O.Firewall. All requirements around the communication control that the TOE poses on communications between the different networks are defined in this policy.
- The **Meter SFP** implements an information flow policy to fulfil the objective O.Meter. It defines all requirements concerning how the TOE shall handle Meter Data.

6.5.2 Gateway Access SFP

6.5.2.1 Access control policy (FDP_ACC)

6.5.2.1.1 FDP_ACC.2: Complete access control

FDP_ACC.2.1 The TSF shall enforce the *Gateway access SFP* [106] on

subjects: external entities in WAN, HAN and LMN

objects: any information that is sent to, from or via the TOE and any information that is stored in the TOE [107] 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.

[106] [assignment: *access control SFP*]

[107] [assignment: *list of subjects and objects*]

Hierarchical to:	FDP_ACC.1 Subset access control
Dependencies:	FDP_ACF.1 Security attribute based access control

6.5.2.1.2 FDP_ACF.1: Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the *Gateway access SFP* [108] to objects based on the following:

subjects: external entities on the WAN, HAN or LMN side

objects: any information that is sent to, from or via the TOE

attributes: destination interface [109].

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

- *an authorised Consumer is only allowed to have read access to his own User Data via the interface IF_GW_CON,*
- *an authorised Service Technician is only allowed to have read access to the system log via the interface IF_GW_SRV, the Service Technician must not be allowed to read, modify or delete any other TSF data,*
- *an authorised Gateway Administrator is allowed to interact with the TOE only via IF_GW_WAN,*
- *only authorised Gateway Administrators are allowed to establish a wake-up call,*
- *additional rules governing access among controlled subjects and controlled objects using controlled*

[108] [assignment: *access control SFP*]

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

operations on controlled objects or none: none [110]. [111]

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none* [112].

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

- *the Gateway Administrator is not allowed to read consumption data or the Consumer Log,*
- *nobody must be allowed to read the symmetric keys used for encryption* [113].

Hierarchical to: No other components

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

6.5.3 Firewall SFP

6.5.3.1 Information flow control policy (FDP_IFC)

6.5.3.1.1 FDP_IFC.2/FW: Complete information flow control for firewall

FDP_IFC.2.1/FW The TSF shall enforce the *Firewall SFP* [114] on *the TOE, external entities on the WAN side, external entities on the LAN side and all information flowing between them* [115] and all operations that cause that information to flow to and from subjects covered by the SFP.

[110] [assignment*: additional rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects or none*]

[111] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]

[112] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]

[113] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

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

[115] [assignment: *list of subjects and information*]

FDP_IFC.2.2/FW 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 Simple security attributes

6.5.3.2 Information flow control functions (FDP_IFF)

6.5.3.2.1 FDP_IFF.1/FW: Simple security attributes for Firewall

FDP_IFF.1.1/FW The TSF shall enforce the *Firewall SFP* [116] based on the following types of subject and information security attributes:

subjects: The TOE and external entities on the WAN, HAN or LMN side

information: any information that is sent to, from or via the TOE

attributes: destination_interface (TOE, LMN, HAN or WAN), source_interface (TOE, LMN, HAN or WAN), destination_authenticated, source_authenticated [117].

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

(if source_interface=HAN or source_interface=TOE) and

destination_interface=WAN and

destination_authenticated = true

Connection establishment is allowed

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

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

```
if source_interface=LMN and
destination_interface= TOE and
source_authenticated = true
        Connection establishment is allowed

if source_interface=TOE and
destination_interface= LMN and
destination_authenticated = true
        Connection establishment is allowed

if source_interface=HAN and
destination_interface= TOE and
source_authenticated = true
        Connection establishment is allowed

if source_interface=TOE and
destination_interface= HAN and
destination_authenticated = true
        Connection establishment is allowed
else
        Connection establishment is denied [118].
```

FDP_IFF.1.3/FW The TSF shall enforce the *establishment of a connection to a configured external entity in the WAN after having received a wake-up message on the WAN interface* [119].

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

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

FDP_IFF.1.4/FW	The TSF shall explicitly authorise an information flow based on the following rules: *none* [120].
FDP_IFF.1.5/FW	The TSF shall explicitly deny an information flow based on the following rules: *none* [121].
Hierarchical to:	No other components
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
Application Note 27:	It should be noted that the FDP_IFF.1.1/FW facilitates different interfaces of the origin and the destination of an information flow implicitly requires the TOE to implement physically separate ports for WAN, LMN and HAN.

6.5.4 Meter SFP

6.5.4.1 Information flow control policy (FDP_IFC)

6.5.4.1.1 FDP_IFC.2/MTR: Complete information flow control for Meter information flow

FDP_IFC.2.1/MTR	The TSF shall enforce the *Meter SFP* [122] on *the TOE, attached Meters, authorized External Entities in the WAN and all information flowing between them* [123] and all operations that cause that information to flow to and from subjects covered by the SFP.
FDP_IFC.2.2/MTR	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 Simple security attributes

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

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

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

[123] [assignment: *list of subjects and information*]

6.5.4.2 Information flow control functions (FDP_IFF)

6.5.4.2.1 FDP_IFF.1/MTR: Simple security attributes for Meter information

FDP_IFF.1.1/MTR

The TSF shall enforce the *Meter SFP*[124] based on the following types of subject and information security attributes:

- *subjects: TOE, external entities in WAN, Meters located in LMN*
- *information: any information that is sent via the TOE*
- *attributes: destination interface, source interface (LMN or WAN), Processing Profile*[125].

FDP_IFF.1.2/MTR

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 only be initiated if allowed by a corresponding Processing Profile*[126]*.*

FDP_IFF.1.3/MTR

The TSF shall enforce the following rules:

- Data received from Meters shall be processed as defined in the corresponding Processing Profiles,
- Results of processing of Meter Data shall be submitted to external entities as defined in the Processing Profiles,
- The internal system time shall be synchronised as follows:

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

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

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

- *The TOE shall compare the system time to a reliable external time source every 24 hours* [127].
- *If the deviation between the local time and the remote time is acceptable* [128]*, the local system time shall be updated according to the remote time.*
- *If the deviation is not acceptable the TOE shall ensure that any following Meter Data is not used, stop operation* [129] *and inform a Gateway Administrator* [130].

FDP_IFF.1.4/MTR The TSF shall explicitly authorise an information flow based on the following rules: *none* [131].

FDP_IFF.1.5/MTR The TSF shall explicitly deny an information flow based on the following rules: *The TOE shall deny any acceptance of information by external entities in the LMN unless the authenticity, integrity and confidentiality of the Meter Data could be verified* [132].

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

Application Note 28: FDP_IFF.1.3 defines that the TOE shall update the local system time regularly with reliable external time sources if the deviation is acceptable. In the context of this functionality two aspects should be mentioned:

[127] [assignment: *synchronization interval between 1 minute and 24 hours*]

[128] Please refer to the following application note for a detailed definition of “acceptable”.

[129] Please note that this refers to the complete functional operation of the TOE and not only to the update of local time. However, an administrative access shall still be possible.

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

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

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

Reliability of external source

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 organisation (an official legal time issued by the calibration authority would be a good example for such a source[133])). 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.

Acceptable deviation

For the question whether a deviation between the time source(s) in the WAN and the local system time is still acceptable, normative or legislative regulations shall be considered. If no regulation exists, a maximum deviation of 3% of the measuring period is allowed to be in conformance with [PP_GW]. It should be noted that depending on the kind of application a more accurate system time is needed. For doing so, the intervall for the comparison of the system time to a reliable external time source is configurable. But this aspect is not within the scope of this Security Target.

Please further note that – depending on the exactness of the local clock – it may be required to synchronize the time more often than every 24 hours.

Application Note 29: In FDP_IFF.1.5/MTR the TOE is required to verify the authenticity, integrity and confidentiality of the Meter Data

[133] By the time that this ST is developed however, this time source is not yet available.

received from the Meter. The TOE has two options to do so:

1. To implement a channel between the Meter and the TOE using the functionality as described in FCS_COP.1/TLS.
2. To accept, decrypt and verify data that has been encrypted by the Meter as required in FCS_COP.1/MTR if a wireless connection to the meters is established.

The latter possibility can be used only if a wireless connection between the Meter and the TOE is established.

6.5.5 General Requirements on user data protection

6.5.5.1 Residual information protection (FDP_RIP)

6.5.5.1.1 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 [134] all objects.

Hierarchical to: FDP_RIP.1 Subset residual information protection

Dependencies: No dependencies.

Application Note 30: Please refer to chapter F.9 of part 2 of [CC] 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

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

way that makes it impossible for an attacker to get access to is assuming a physical access to the memory of the TOE.

6.5.5.2 Stored data integrity (FDP_SDI)

6.5.5.2.1 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 *integrity errors* [135] on all objects, based on the following attributes: *cryptographical check sum* [136].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall *create a system log entry*[137].

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

Dependencies: No dependencies.

6.6 Class FIA: Identification and Authentication

6.6.1 User Attribute Definition (FIA_ATD)

6.6.1.1 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*
- *none* [138].

Hierarchical to: No other components.

Dependencies: No dependencies.

[135] [assignment: *integrity errors*]

[136] [assignment: *user data attributes*]

[137] [assignment: *action to be taken*]

[138] [assignment: *list of security attributes*]

6.6.2 Authentication Failures (FIA_AFL)

6.6.2.1 FIA_AFL.1: Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when 5[139] unsuccessful authentication attempts occur related to *authentication attempts at IF_GW_CON*[140].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met[141], the TSF shall *block IF_GW_CON for 5 minutes*[142].

Hierarchical to: No other components

Dependencies: FIA_UAU.1 Timing of authentication

6.6.3 User Authentication (FIA_UAU)

6.6.3.1 FIA_UAU.2: User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Hierarchical to: FIA_UAU.1

Dependencies: FIA_UID.1 Timing of identification

Application Note 31: Please refer to [TR-03109-1] for a more detailed overview on the authentication of TOE users.

6.6.3.2 FIA_UAU.5: Multiple authentication mechanisms

FIA_UAU.5.1 The TSF shall provide

- *authentication via certificates at the IF_GW_MTR interface*
- *TLS-authentication via certificates at the IF_GW_WAN interface*

[139] [selection: *[assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]*]

[140] [assignment: *list of authentication events*]

[141] [selection: *met*, *surpassed*]

[142] [assignment: *list of actions*]

- *TLS-authentication via HAN-certificates at the IF_GW_CON interface*
- *authentication via password at the IF_GW_CON interface*
- *TLS-authentication via HAN-certificates at the IF_GW_SRV interface*
- *authentication at the IF_GW_CLS interface*
- *verification via a commands' signature* [143]

to support user authentication.

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

- *meters shall be authenticated via certificates at the IF_GW_MTR interface only*
- *Gateway Administrators shall be authenticated via TLS-certificates at the IF_GW_WAN interface only*
- *Consumers shall be authenticated via TLS-certificates or via password at the IF_GW_CON interface only*
- *Service Technicians shall be authenticated via TLS-certificates at the IF_GW_SRV interface only*
- *CLS shall be authenticated at the IF_GW_CLS only*
- *each command of an Gateway Administrator shall be authenticated by verification of the commands' signature,*
- *other external entities shall be authenticated via TLS-certificates at the IF_GW_WAN interface only* [144].

[143] [assignment: *list of multiple authentication mechanisms*]

[144] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 32: Please refer to [TR-03109-1] for a more detailed overview on the authentication of TOE users.

6.6.3.3 FIA_UAU.6: Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate **an external entity** [145] under the conditions

- *TLS channel to the WAN shall be disconnected after 48 hours,*
- *TLS channel to the LMN shall be disconnected after 5 MB of transmitted information,*
- *other local users shall be re-authenticated after at least 10 minutes*[146] *of inactivity* [147]*.*

Hierarchical to: No other components.

Dependencies: No dependencies.

***A**pplication Note 33*: This requirement on re-authentication for external entities in the WAN and LMN is addressed by disconnecting the TLS channel even though a re-authentication is - strictly speaking - only achieved if the TLS channel is build up again.

6.6.4 User identification (FIA_UID)

6.6.4.1 FIA_UID.2: User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Hierarchical to: FIA_UID.1

Dependencies: No dependencies.

[145] [refinement: *the user*]

[146] [refinement: *after **at least** 10 minutes*]. This value is configurable by the authorised Gateway Administrator.

[147] [assignment: *list of conditions under which re-authentication is required*]

6.6.5 User-subject binding (FIA_USB)

6.6.5.1 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* [148].

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:

- *The initial value of the security attribute 'connecting network' is set to the corresponding physical interface of the TOE (HAN, WAN, or LMN).*
- *The initial value of the security attribute 'role membership' is set to the user role claimed on basis of the credentials used for authentication at the connecting network as defined in FIA_UAU.5.2. For role membership 'Gateway Administrators', additionally the remote network endpoint* [149]*used and configured in the TSF data must be identical.*
- *The initial value of the security attribute 'user identity' is set to the identification attribute of the credentials used by the subject. The security attribute 'user identity' is set to the subject key ID of the certificate in case of a certificate-based authentication, the meter-ID for wired Meters and the user name owner in case of a password-based authentication at interface IF_GW_CON.*
- *The initial value of the security attribute 'status of identity' is set to the authentication status of the claimed identity. If the authentication is successful on basis of the used credentials, the status of*

[148] [assignment: *list of user security attributes*]

[149] The remote network endpoint can be either the remote IP address or the remote host name.

identity is ‘authenticated’, otherwise it is ‘not authenticated’ [150].

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:

- *security attribute ‘connecting network’ is not changeable.*
- *security attribute ‘role membership’ is not changeable.*
- *security attribute ‘user identity’ is not changeable.*
- *security attribute ‘status of identity’ is not changeable*[151].

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

6.7 Class FMT: Security Management

6.7.1 Management of the TSF

6.7.1.1 Management of functions in TSF (FMT_MOF)

6.7.1.1.1 FMT_MOF.1: Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to modify the behaviour of [152] the functions *for management as defined in*

[150] [assignment: *rules for the initial association of attributes*]

[151] [assignment: *rules for the changing of attributes*]

[152] [selection: *determine the behaviour of*, *disable*, *enable*, *modify the behaviour of*]

FMT_SMF.1 [153] to *roles and criteria as defined in Table 13* [154].

Hierarchical to: No other components.

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

Function	**Limitation**
Display the version number of the TOE Display the current time	The management functions must only be accessible for an authorised Consumer and only via the interface IF_GW_CON. **An authorized Service Technician is also able to access the version numer of the TOE and the current time of the TOE via interface IF_GW_SRV** [155].
All other management functions as defined in FMT_SMF.1	The management functions must only be accessible for an authorised Gateway Administrator and only via the interface IF_GW_WAN [156].
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 Gateway developer) and if the version number of the new firmware is higher to the version of the installed firmware.
Deletion or modification of events from the Calibration Log	A deletion or modification of events from the calibration log must not be possible.

Table 13: Restrictions on Management Functions

[153] [assignment: *list of functions*]

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

[155] The TOE displays the version number of the TOE and the current time of the TOE also to the authorized service technician via the interface IF_GW_SRV because the service technician must be able to determine if the current time of the TOE is correct or if the version number of the TOE is correct.

[156] This criterion applies to all management functions. The following entries in this table only augment this restriction further.

6.7.1.2 Specification of Management Functions (FMT_SMF)

6.7.1.2.1 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 14 and Table 15 and additional functionalities: none* [157].
Hierarchical to:	No other components.
Dependencies:	No dependencies.

SFR	Management functionality
FAU_ARP.1/SYS	~~• **The management (addition, removal, or modification) of actions**~~ [158]
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**~~ [158]
FAU_SAR.1/SYS FAU_SAR.1/CON FAU_SAR.1/CAL	- [159]
FAU_STG.4/SYS FAU_STG.4/CON	~~• **Maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure**~~ [158] • ~~**Size configuration of the audit trail that is available before the oldest events get overwritten**~~ [158]

[157] [assignment: *list of management functions to be provided by the TSF*]

[158] The TOE does not have the indicated management ability since there exist no standard method calls for the Gateway Administrator to enforce such management ability.

[159] As the rules for audit review are fixed within [PP_GW], the management functions as defined by [CC, part 2] do not apply.

FAU_STG.4/CAL	- [160]
FAU_GEN.2	-
FAU_STG.2	• Maintenance of the parameters that control the audit storage capability for the consumer log ~~and the system log~~ [158]
FCO_NRO.2	• The management of changes to ~~information types, fields,~~ [158] originator attributes and recipients of evidence
FCS_CKM.1/TLS	-
FCS_COP.1/TLS	• Management of key material including key material stored in the Security Module
FCS_CKM.1/CMS	-
FCS_COP.1/CMS	• Management of key material including key material stored in the Security Module
FCS_CKM.1/MTR	-
FCS_COP.1/MTR	• Management of key material stored in the Security Module and key material brought into the gateway during the pairing process
FCS_CKM.4	-
FCS_COP.1/HASH	-
FCS_COP.1/MEM	~~• Management of key material~~
FDP_ACC.2	-
FDP_ACF.1	-
FDP_IFC.2/FW	-

[160] As the actions that shall be performed if the audit trail is full are fixed within [PP_GW], the management functions as defined by [CC, part 2] do not apply.

FDP_IFF.1/FW	• Managing the attributes used to make explicit access based decisions • Add authorised units for communication (pairing) • Management of endpoint to be contacted after successful wake-up call • Management of CLS systems
FDP_IFC.2/MTR	-
FDP_IFF.1/MTR	• Managing the attributes (including Processing Profiles) used to make explicit access based decisions
FDP_RIP.2	-
FDP_SDI.2	• ~~**The actions to be taken upon the detection of an integrity error shall be configurable.**~~ [158]
FIA_ATD.1	• If so indicated in the assignment, the authorised Gateway Administrator might be able to define additional security attributes for users[161].
FIA_AFL.1	• ~~**Management of the threshold for unsuccessful authentication attempts**~~ [158] • ~~**Management of actions to be taken in the event of an authentication failure**~~ [158]
FIA_UAU.2	• Management of the authentication data by an Gateway Administrator
FIA_UAU.5	- [162]
FIA_UAU.6	• Management of re-authentication time

[161] In the assignment it is not indicated that the authorized Gateway Administrator might be able to define additional security attributes for users.

[162] As the rules for re-authentication are fixed within [PP_GW], the management functions as defined by [CC, part 2] do not apply.

FIA_UID.2	• The management of the user identities
FIA_USB.1	• ~~**An authorised Gateway Administrator can define default subject security attributes, if so indicated in the assignment of FIA_ATD.1.**~~[158] • ~~**An authorised Gateway Administrator can change subject security attributes, if so indicated in the assignment of FIA_ATD.1.**~~[158]
FMT_MOF.1	• ~~**Managing the group of roles that can interact with the functions in the TSF**~~
FMT_SMF.1	-
FMT_SMR.1	• Managing the group of users that are part of a role
FMT_MSA.1/AC	• ~~**Management of rules by which security attributes inherit specified values**~~ [163][158]
FMT_MSA.3/AC	- [164]
FMT_MSA.1/FW	• ~~**Management of rules by which security attributes inherit specified values**~~ [165][158]
FMT_MSA.3/FW	- [166]
FMT_MSA.1/MTR	• ~~**Management of rules by which security attributes inherit specified values**~~ [167][158]

[163] As the role that can interact with the security attributes is restricted to the Gateway Administrator within [PP_GW], not all management functions as defined by [CC, part 2] do apply.

[164] As no role is allowed to specify alternative initial values within [PP_GW], the management functions as defined by [CC, part 2] do not apply.

[165] As the role that can read, modify, delete or add the security attributes is restricted to the Gateway Administrator within [PP_GW], not all management functions as defined by [CC, part 2] do apply.

[166] As no role is allowed to specify alternative initial values within [PP_GW], the management functions as defined by [CC, part 2] do not apply.

[167] As the role that can read, modify, delete or add the security attributes is restricted to the Gateway Administrator within [PP_GW], not all management functions as defined by [CC, part 2] do apply.

FMT_MSA.3/MTR	- [168]
FPR_CON.1	~~• **Definition of the interval in FPR_CON.1.2 if definable within the operational phase of the TOE**~~ [158]
FPR_PSE.1	-
FPT_FLS.1	-
FPT_RPL.1	-
FPT_STM.1	• Management a time source
FPT_TST.1	- [169]
FPT_PHP.1	~~• **Management of the user or role that determines whether physical tampering has occurred**~~ [158]
FTP_ITC.1/WAN	- [170]
FTP_ITC.1/MTR	- [171]
FTP_ITC.1/USR	- [172]

2203 **Table 14: SFR related Management Functionalities**

[168] As no role is allowed to specify alternative initial values within [PP_GW], the management functions as defined by [CC, part 2] do not apply.

[169] As the rules for TSF testing are fixed within [PP_GW], the management functions as defined by [CC, part 2] do not apply.

[170] As the configuration of the actions that require a trusted channel is fixed by [PP_GW], the management functions as defined in [CC, part 2] do not apply.

[171] As the configuration of the actions that require a trusted channel is fixed by [PP_GW], the management functions as defined in [CC, part 2] do not apply.

[172] As the configuration of the actions that require a trusted channel is fixed by [PP_GW], the management functions as defined in [CC, part 2] do not apply.

Gateway specific Management functionality
Pairing of a Meter
Performing a firmware update
Displaying the current version number of the TOE
Displaying the current time
Management of certificates of external entities in the WAN for communication
Resetting of the TOE [173]

Table 15: Gateway specific Management Functionalities

6.7.2 Security management roles (FMT_SMR)

6.7.2.1 FMT_SMR.1: Security roles

FMT_SMR.1.1 The TSF shall maintain the roles *authorised Consumer, authorised Gateway Administrator, authorised Service Technician, the authorised identified roles: authorised external entity, CLS, and Meter* [174].

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

Hierarchical to: No other components.

Dependencies: No dependencies.

[173] Resetting the TOE will be necessary when the TOE stopped operation due to a critical deviation between local and remote time (see FDP_IFF.1.3/MTR)~~or when the calibration log is full.~~

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

6.7.3 Management of security attributes for Gateway access SFP

6.7.3.1 Management of security attributes (FMT_MSA)

6.7.3.1.1 FMT_MSA.1/AC: Management of security attributes for Gateway access SFP

FMT_MSA.1.1/AC	The TSF shall enforce the *Gateway access SFP* [175] to restrict the ability to <u>query, modify, delete, other operations: none</u> [176] the security attributes *all relevant security attributes* [177] to *authorised Gateway Administrators* [178].
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], fulfilled by FDP_ACC.2 FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

6.7.3.1.2 FMT_MSA.3/AC: Static attribute initialisation for Gateway access SFP

FMT_MSA.3.1/AC	The TSF shall enforce the *Gateway access SFP* [179] to provide <u>restrictive</u> [180] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/AC	The TSF shall allow the *no role* [181] to specify alternative initial values to override the default values when an object or information is created.

[175] [assignment: *access control SFP(s), information flow control SFP(s)*]

[176] [selection: *change_default*, *query*, *modify*, *delete*, *[assignment: other operations]*]

[177] [assignment: *list of security attributes*]

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

[179] [assignment: *access control SFP, information flow control SFP*]

[180] [selection, choose one of: *restrictive*, *permissive*, *[assignment: other property]*]

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

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

6.7.4 Management of security attributes for Firewall SFP

6.7.4.1 Management of security attributes (FMT_MSA)

6.7.4.1.1 FMT_MSA.1/FW: Management of security attributes for firewall policy

FMT_MSA.1.1/FW The TSF shall enforce the *Firewall SFP* [182] to restrict the ability to query, modify, delete, other operations: none [183] the security attributes *all relevant security attributes* [184] to *authorised Gateway Administrators* [185].

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control], fulfilled by FDP_IFC.2/FW

FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

6.7.4.1.2 FMT_MSA.3/FW: Static attribute initialisation for Firewall policy

FMT_MSA.3.1/FW The TSF shall enforce the *Firewall SFP* [186] to provide restrictive [187] default values for security attributes that are used to enforce the SFP.

[182] [assignment: *access control SFP(s), information flow control SFP(s)*]

[183] [selection: *change_default*, *query*, *modify*, *delete*, *[assignment: other operations]*]

[184] [assignment: *list of security attributes*]

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

[186] [assignment: *access control SFP, information flow control SFP*]

[187] [selection, choose one of: *restrictive*, *permissive*, *[assignment: other property]*]

FMT_MSA.3.2/FW The TSF shall allow the *no role* [188] to specify alternative initial values to override the default values when an object or information is created.

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

Application Note 34: The definition of restrictive default rules for the firewall information flow policy refers to the rules as defined in FDP_IFF.1.2/FW and FDP_IFF.1.5/FW. Those rules apply to all information flows and must not be overwritable by anybody.

6.7.5 Management of security attributes for Meter SFP

6.7.5.1 Management of security attributes (FMT_MSA)

6.7.5.1.1 FMT_MSA.1/MTR: Management of security attributes for Meter policy

FMT_MSA.1.1/MTR The TSF shall enforce the *Meter SFP* [189] to restrict the ability to change_default, query, modify, delete, other operations: none [190] the security attributes *all relevant security attributes* [191] to *authorised Gateway Administrators* [192].

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control], fulfilled by FDP_IFC.2/FW

FMT_SMR.1 Security roles

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

[189] [assignment: *access control SFP(s), information flow control SFP(s)*]

[190] [selection: *change_default*, *query*, *modify*, *delete*, *[assignment: other operations]*]

[191] [assignment: *list of security attributes*]

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

FMT_SMF.1 Specification of Management Functions

6.7.5.1.2 FMT_MSA.3/MTR: Static attribute initialisation for Meter policy

FMT_MSA.3.1/MTR The TSF shall enforce the *Meter SFP* [193] to provide <u>restrictive</u> [194] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/MTR The TSF shall allow the *no role* [195] to specify alternative initial values to override the default values when an object or information is created.

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

6.8 Class FPR: Privacy

6.8.1 Communication Concealing (FPR_CON)

6.8.1.1 FPR_CON.1: Communication Concealing

FPR_CON.1.1 The TSF shall enforce the *Firewall SFP* [196] in order to ensure that no personally identifiable information (PII) can be obtained by an analysis of *frequency, load, size or the absence of external communication* [197].

FPR_CON.1.2 The TSF shall connect to *the Gateway Administrator, authorized External Entity in the WAN* [198] in intervals as

[193] [assignment: *access control SFP, information flow control SFP*]

[194] [selection, choose one of: *restrictive*, *permissive*, *[assignment: other property]*]

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

[196] [assignment: *information flow policy*]

[197] [assignment: *characteristics of the information flow that need to be concealed*]

[198] [assignment: *list of external entities*]

follows daily, other interval: none [199] to conceal the data flow[200].

Hierarchical to: No other components.

Dependencies: No dependencies.

6.8.2 Pseudonymity (FPR_PSE)

6.8.2.1 FPR_PSE.1 Pseudonymity

FPR_PSE.1.1 The TSF shall ensure that *external entities in the WAN* [201] are unable to determine the real user name bound to *information neither relevant for billing nor for a secure operation of the Grid sent to parties in the WAN* [202].

FPR_PSE.1.2 The TSF shall be able to provide *aliases as defined by the Processing Profiles* [203] ~~**of the real user name**~~ **for the Meter and Gateway identity** [204] to *external entities in the WAN* [205].

FPR_PSE.1.3 The TSF shall determine an alias for a user [206] and verify that it conforms to the *alias given by the Gateway Administrator in the Processing Profile*[207].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 35: 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 Grid, there is no need that this information is sent with a direct

[199] [selection: *weekly, daily*, *hourly*, *[assignment: other interval]*]

[200] The TOE uses a randomized value of about ±50 percent per delivery.

[201] [assignment: *set of users and/or subjects*]

[202] [assignment: *list of subjects and/or operations and/or objects*]

[203] [assignment: *number of aliases*]

[204] [refinement: *of the real user name*]

[205] [assignment: *list of subjects*]

[206] [selection, choose one of: *determine an alias for a user*, *accept the alias from the user*]

[207] [assignment: *alias metric*]

link to the identity of the consumer. In those cases, the TOE shall replace the identity of the Consumer by a pseudonymous identifier. Please note that the identity of the Consumer may not be their name but could also be a number (e.g. consumer ID) used for billing purposes.

A Gateway may use more than one pseudonymous identifier.

A complete anonymisation would be beneficial in terms of the privacy of the consumer. However, a complete anonymous set of information would not allow the external entity to ensure that the data comes from a trustworthy source.

Please note that an information flow shall only be initiated if allowed by a corresponding Processing Profile.

6.9 Class FPT: Protection of the TSF

6.9.1 Fail secure (FPT_FLS)

6.9.1.1 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:

- *the deviation between local system time of the TOE and the reliable external time source is too large,*
- *TOE hardware / firmware integrity violation or*
- *TOE software application integrity violation* [208].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 36: The local clock shall be as exact as required by normative or legislative regulations. If no regulation exists, a

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

maximum deviation of 3% of the measuring period is allowed to be in conformance with [PP_GW].

6.9.2 Replay Detection (FPT_RPL)

6.9.2.1 FPT_RPL.1: Replay detection

FPT_RPL.1.1 The TSF shall detect replay for the following entities: *all external entities* [209].

FPT_RPL.1.2 The TSF shall perform *ignore replayed data* [210] when replay is detected.

Hierarchical to: No other components.

Dependencies: No dependencies.

6.9.3 Time stamps (FPT_STM)

6.9.3.1 FPT_STM.1: Reliable time stamps

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

Hierarchical to: No other components.

Dependencies: No dependencies.

6.9.4 TSF self test (FPT_TST)

6.9.4.1 FPT_TST.1: TSF testing

FPT_TST.1.1 The TSF shall run a suite of self tests during initial startup, at the request of a user and periodically during normal operation [211] to demonstrate the correct operation of the TSF [212].

[209] [assignment: *list of identified entities*]

[210] [assignment: *list of specific actions*]

[211] [selection: *during initial start-up*, *periodically during normal operation*, *at the request of the authorised user*, *at the conditions[assignment: conditions under which self test should occur]*]

[212] [selection: *[assignment: parts of TSF], the TSF*]

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of TSF data [213].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of TSF [214].

Hierarchical to: No other components.

Dependencies: No dependencies.

6.9.5 TSF physical protection (FPT_PHP)

6.9.5.1 FPT_PHP.1: Passive detection of physical attack

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might 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 elements has occurred.

Hierarchical to: No other components.

Dependencies: No dependencies.

6.10 Class FTP: Trusted path/channels

6.10.1 Inter-TSF trusted channel (FTP_ITC)

6.10.1.1 FTP_ITC.1/WAN: Inter-TSF trusted channel for WAN

FTP_ITC.1.1/WAN The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

[213] [selection: *[assignment: parts of TSF data], TSF data*]

[214] [selection: *[assignment: parts of TSF], TSF*]

FTP_ITC.1.2/WAN The TSF shall permit the TSF [215] to initiate communication via the trusted channel.

FTP_ITC.1.3/WAN The TSF shall initiate communication via the trusted channel for *all communications to external entities in the WAN* [216].

Hierarchical to: No other components

Dependencies: No dependencies.

6.10.1.2 FTP_ITC.1/MTR: Inter-TSF trusted channel for Meter

FTP_ITC.1.1/MTR The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/MTR The TSF shall permit **the Meter and the TOE** [217] to initiate communication via the trusted channel.

FTP_ITC.1.3/MTR The TSF shall initiate communication via the trusted channel for *any communication between a Meter and the TOE* [218].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 37: The corresponding cryptographic primitives are defined by FCS_COP.1/MTR.

6.10.1.3 FTP_ITC.1/USR: Inter-TSF trusted channel for User

FTP_ITC.1.1/USR The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured

[215] [selection: *the TSF*, *another trusted IT product*]

[216] [assignment: *list of functions for which a trusted channel is required*]

[217] [selection: *the TSF*, *another trusted IT product*]

[218] [assignment: *list of functions for which a trusted channel is required*]

identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/USR The TSF shall permit **the Consumer, the Service Technician** [219] to initiate communication via the trusted channel.

FTP_ITC.1.3/USR The TSF shall initiate communication via the trusted channel for *any communication between a Consumer and the TOE and the Service Technician and the TOE* [220].

Hierarchical to: No other components.

Dependencies: No dependencies.

6.11 Security Assurance Requirements for the TOE

The minimum Evaluation Assurance Level for this Security Target 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 ST.

Assurance Class	Assurance Component
Development	ADV_ARC.1
	ADV_FSP.4
	ADV_IMP.1
	ADV_TDS.3
Guidance documents	AGD_OPE.1
	AGD_PRE.1
Life-cycle support	ALC_CMC.4

[219] [selection: *the TSF*, *another trusted IT product*]

[220] [assignment: *list of functions for which a trusted channel is required*]

Assurance Class	**Assurance Component**
	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**

2445 **Table 16: Assurance Requirements**

6.12 Security Requirements rationale

6.12.1 Security Functional Requirements rationale

6.12.1.1 Fulfilment of the Security Objectives

This chapter proves that the set of security requirements (TOE) is suited to fulfil 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.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Manage-	O.Log	O.Access
FAU_ARP.1/SYS									X	
FAU_GEN.1/SYS									X	
FAU_SAA.1/SYS									X	
FAU_SAR.1/SYS									X	
FAU_STG.4/SYS									X	
FAU_GEN.1/CON									X	
FAU_SAR.1/CON									X	
FAU_STG.4/CON									X	
FAU_GEN.1/CAL									X	
FAU_SAR.1/CAL									X	
FAU_STG.4/CAL									X	
FAU_GEN.2									X	
FAU_STG.2									X	
FCO_NRO.2				X						

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Manage-	O.Log	O.Access
FCS_CKM.1/TLS					X					
FCS_COP.1/TLS					X					
FCS_CKM.1/CMS					X					
FCS_COP.1/CMS					X					
FCS_CKM.1/MTR					X					
FCS_COP.1/MTR					X					
FCS_CKM.4					X					
FCS_COP.1/HASH					X					
FCS_COP.1/MEM					X		X			
FDP_ACC.2										X
FDP_ACF.1										X
FDP_IFC.2/FW	X	X								
FDP_IFF.1/FW	X	X								
FDP_IFC.2/MTR				X		X				
FDP_IFF.1/MTR				X		X				
FDP_RIP.2							X			
FDP_SDI.2							X			
FIA_ATD.1								X		

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Manage-	O.Log	O.Access
FIA_AFL.1								X		
FIA_UAU.2								X		
FIA_UAU.5										X
FIA_UAU.6										X
FIA_UID.2								X		
FIA_USB.1								X		
FMT_MOF.1								X		
FMT_SMF.1								X		
FMT_SMR.1								X		
FMT_MSA.1/AC								X		
FMT_MSA.3/AC								X		
FMT_MSA.1/FW								X		
FMT_MSA.3/FW								X		
FMT_MSA.1/MTR								X		
FMT_MSA.3/MTR								X		
FPR_CON.1			X							
FPR_PSE.1				X						
FPT_FLS.1							X			

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Manage-	O.Log	O.Access
FPT_RPL.1					X					
FPT_STM.1						X			X	
FPT_TST.1		X					X			
FPT_PHP.1							X			
FTP_ITC.1/WAN	X									
FTP_ITC.1/MTR				X						
FTP_ITC.1/USR									X	

Table 17: Fulfilment of Security Objectives

The following paragraphs contain more details on this mapping.

6.12.1.1.1 O.Firewall

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

- **FDP_IFC.2/FW** defines that the TOE shall implement an information flow policy for its firewall functionality.
- **FDP_IFF.1/FW** defines the concrete rules for the firewall information flow policy.
- **FTP_ITC.1/WAN** defines the policy around the trusted channel to parties in the WAN.

6.12.1.1.2 O.SeparateIF

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

- **FDP_IFC.2/FW** and **FDP_IFF.1/FW** implicitly require the TOE to implement physically separate ports for WAN and LMN.
- **FPT_TST.1** implements a self test that also detects whether the ports for WAN and LAN have been interchanged.

6.12.1.1.3 O.Conceal

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

6.12.1.1.4 O.Meter

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

- **FDP_IFC.2/MTR** and **FDP_IFF.1/MTR** define an information flow policy to introduce how the Gateway shall handle Meter Data.
- **FCO_NRO.2** ensure that all Meter Data will be signed by the Gateway (invoking the services of its Security Module) before being submitted to external entities.
- **FPR_PSE.1** defines requirements around the pseudonymization of Meter identities for Status data.
- **FTP_ITC.1/MTR** defines the requirements around the Trusted Channel that shall be implemented by the Gateway in order to protect information submitted via the Gateway and external entities in the WAN or the Gateway and a distributed Meter.

6.12.1.1.5 O.Crypt

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

- **FCS_CKM.4** defines the requirements around the secure deletion of ephemeral cryptographic keys.
- **FCS_CKM.1/TLS** defines the requirements on key negotiation for the TLS protocol.
- **FCS_CKM.1/CMS** defines the requirements on key generation for symmetric encryption within CMS.
- **FCS_COP.1/TLS** defines the requirements around the encryption and decryption capabilities of the Gateway for communications with external parties and to Meters.
- **FCS_COP.1/CMS** defines the requirements around the encryption and decryption of content and administration data.
- **FCS_CKM.1/MTR** defines the requirements on key negotiation for meter communication encryption.
- **FCS_COP.1/MTR** defines the cryptographic primitives for meter communication encryption.
- **FCS_COP.1/HASH** defines the requirements on hashing that are needed in the context of digital signatures (which are created and verified by the Security Module).
- **FCS_COP.1/MEM** defines the requirements around the encryption of TSF data.
- **FPT_RPL.1** ensures that a replay attack for communications with external entities is detected.

6.12.1.1.6 O.Time

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

- **FDP_IFC.2/MTR** and **FDP_IFF.1/MTR** define the required update functionality for the local time as part of the information flow control policy for handling Meter Data.
- **FPT_STM.1** defines that the TOE shall be able to provide reliable time stamps.

6.12.1.1.7 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 data.
- **FPT_FLS.1** defines requirements that the TOE falls back to a safe state for specific error cases.
- **FPT_TST.1** defines the self testing functionality to detect whether the interfaces for WAN and LAN are separate.
- **FPT_PHP.1** defines the exact requirements around the physical protection that the TOE has to provide.

6.12.1.1.8 O.Management

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

- **FIA_ATD.1** defines the attributes for users.
- **FIA_AFL.1** defines the requirements if the authentication of users fails multiple times.
- **FIA_UAU.2** defines requirements around the authentication of users.
- **FIA_UID.2** defines requirements around the identification of users.
- **FIA_USB.1** defines that the TOE must be able to associate users with subjects acting on behalf of them.
- **FMT_MOF.1** defines requirements around the limitations for management of security functions.
- **FMT_MSA.1/AC** defines requirements around the limitations for management of attributes used for the Gateway access SFP.
- **FMT_MSA.1/FW** defines requirements around the limitations for management of attributes used for the Firewall SFP.
- **FMT_MSA.1/MTR** defines requirements around the limitations for management of attributes used for the Meter SFP.
- **FMT_MSA.3/AC** defines the default values for the Gateway access SFP.
- **FMT_MSA.3/FW** defines the default values for the Firewall SFP.
- **FMT_MSA.3/MTR** defines the default values for the Meter SFP.

- **FMT_SMF.1** defines the management functionalities that the TOE must offer.
- **FMT_SMR.1** defines the role concept for the TOE.

6.12.1.1.9 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 around the audit review functions and that access to them shall be limited to authorised Gateway Administrators via the IF_GW_WAN interface and to authorised Service Technicians via the IF_GW_SRV interface. Finally, **FAU_STG.4/SYS** defines the requirements on what should happen if the audit log is full.

Consumer Log

The implementation of the consumer log itself is covered by the use of **FAU_GEN.1/CON**. **FAU_STG.4/CON** defines the requirements on what should happen if the audit log is full. **FAU_SAR.1/CON** defines the requirements around the audit review functions for the consumer log and that access to them shall be limited to authorised Consumer via the IF_GW_CON interface. **FTP_ITC.1/USR** 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.4/CAL** defines the requirements on what should happen if the audit log is full. **FAU_SAR.1/CAL** defines the requirements around the audit review functions for the calibration log and that access to them shall be limited to authorised Gateway Administrators via the IF_GW_WAN interface.

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

6.12.1.1.10 O.Access

FDP_ACC.2 and **FDP_ACF.1** define the access control policy as required to address O.Access. **FIA_UAU.5** ensures that entities that would like to communicate with the TOE are authenticated before any action whereby **FIA_UAU.6** ensures that external entities in the WAN are re-authenticated after the session key has been used for a certain amount of time.

6.12.1.2 Fulfilment of the dependencies

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

SFR	Dependencies	Fulfilled by
FAU_ARP.1/SYS	FAU_SAA.1 Potential violation analysis	FAU_SAA.1/SYS
FAU_GEN.1/SYS	FPT_STM.1 Reliable time stamps	FPT_STM.1
FAU_SAA.1/SYS	FAU_GEN.1 Audit data generation	FAU_GEN.1/SYS
FAU_SAR.1/SYS	FAU_GEN.1 Audit data generation	FAU_GEN.1/SYS
FAU_STG.4/SYS	FAU_STG.1 Protected audit trail storage	FAU_STG.2
FAU_GEN.1/CON	FPT_STM.1 Reliable time stamps	FPT_STM.1
FAU_SAR.1/CON	FAU_GEN.1 Audit data generation	FAU_GEN.1/CON
FAU_STG.4/CON	FAU_STG.1 Protected audit trail storage	FAU_STG.2
FAU_GEN.1/CAL	FPT_STM.1 Reliable time stamps	FPT_STM.1
FAU_SAR.1/CAL	FAU_GEN.1 Audit data generation	FAU_GEN.1/CAL
FAU_STG.4/CAL	FAU_STG.1 Protected audit trail storage	FAU_STG.2
FAU_GEN.2	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification	FAU_GEN.1/SYS FAU_GEN.1/CON FIA_UID.2
FAU_STG.2	FAU_GEN.1 Audit data generation	FAU_GEN.1/SYS FAU_GEN.1/CON FAU_GEN.1/CAL

FCO_NRO.2	FIA_UID.1 Timing of identification	FIA_UID.2
FCS_CKM.1/TLS	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/TLS FCS_CKM.4
FCS_COP.1/TLS	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/TLS FCS_CKM.4
FCS_CKM.1/CMS	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/CMS FCS_CKM.4
FCS_COP.1/CMS	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/CMS FCS_CKM.4
FCS_CKM.1/MTR	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/MTR FCS_CKM.4
FCS_COP.1/MTR	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or	FCS_CKM.1/TLS FCS_CKM.4

	FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	FCS_CKM.1/TLS FCS_CKM.1/CMS FCS_CKM.1/MTR
FCS_COP.1/HASH	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Please refer to chapter 6.12.1.3 for missing dependency FCS_CKM.4
FCS_COP.1/MEM	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	not fulfilled [221] FCS_CKM.4
FDP_ACC.2	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.2 FMT_MSA.3/AC
FDP_IFC.2/FW	FDP_IFF.1 Simple security attributes	FDP_IFF.1/FW

[221] The key will be generated by secure production environment and not the TOE itself.

FDP_IFF.1/FW	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	FDP_IFC.2/FW FMT_MSA.3/FW
FDP_IFC.2/MTR	FDP_IFF.1 Simple security attributes	FDP_IFF.1/MTR
FDP_IFF.1/MTR	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	FDP_IFC.2/MTR FMT_MSA.3/MTR
FDP_RIP.2	-	-
FDP_SDI.2	-	-
FIA_ATD.1	-	-
FIA_AFL.1	FIA_UAU.1 Timing of authentication	FIA_UAU.2
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UAU.5	-	-
FIA_UAU.6	-	-
FIA_UID.2	-	-
FIA_USB.1	FIA_ATD.1 User attribute definition	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	-	-
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2
FMT_MSA.1/AC	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles	FDP_ACC.2 FMT_SMR.1 FMT_SMF.1

	FMT_SMF.1 Specification of Management Functions	
FMT_MSA.3/AC	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1/AC FMT_SMR.1
FMT_MSA.1/FW	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_IFC.2/WAN FMT_SMR.1 FMT_SMF.1
FMT_MSA.3/FW	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1/FW FMT_SMR.1
FMT_MSA.1/MTR	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_IFC.2/MTR FMT_SMR.1 FMT_SMF.1
FMT_MSA.3/MTR	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1/MTR FMT_SMR.1
FPR_CON.1	-	-
FPR_PSE.1	-	-
FPT_FLS.1	-	-
FPT_RPL.1	-	-
FPT_STM.1	-	-
FPT_TST.1	-	-

FPT_PHP.1	-	-
FTP_ITC.1/WAN	-	-
FTP_ITC.1/MTR	-	-
FTP_ITC.1/USR	-	-

Table 18: SFR Dependencies

6.12.1.3 Justification for missing dependencies

Dependency FCS_CKM.1 for FCS_COP.1/MEM ist not fulfilled. For the key generation process an external security module (“D-HSM”) is used so that the key is imported from an HSM during TOE production.

The hash algorithm as defined in FCS_COP.1/HASH does not need any key material. As such the dependency to an import or generation of key material is omitted for this SFR.

6.12.2 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 Security Target 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 Security Target commercially feasible EAL 4 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.

6.12.2.1 Dependencies of assurance components

The dependencies of the assurance requirements taken from EAL 4 are fulfilled automatically. The augmentation by AVA_VAN.5 and ALC_FLR.2 does not introduce additional assurance components that are not contained in EAL 4.

7 TOE Summary Specification

The following paragraph provides a TOE summary specification describing how the TOE meets each SFR.

7.1 SF.1: Authentication of Communication and Role Assignment for external entities

The TOE contains a software module that authenticates all communication channels with WAN, HAN and LMN networks. The authentication is based on the TLS 1.2 protocol compliant to [RFC 5246]. According to [TR-03109], this TLS authentication mechanism is used for all TLS secured communications channels with external entities. The TOE does always implement the bidirectional authentication as required by [TR-03109-1] with one exception: if the Consumer requests a password-based authentication from the GWA according to [TR-03109-1], and the GWA activates this authentication method for this Consumer, the TOE uses a unidirectional TLS authentication. Thus, although the client has not sent a valid certificate, the TOE continues the TLS authentication process with the password authentication process for this client (see [RFC 5246, chap. 7.4.6.]). The password policy to be fulfilled hereby is that the password must be at least 10 characters long containing at least one character of each of the following character groups: capital letters, small letters, digits, and special characters (!"§$%&/()=?+*~#',;.:-_). Further characters could also be used.

[TR-03109-1] requires the TOE to use elliptical curves conforming to [RFC 5289] whereas the following cipher suites are supported:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, and
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384.

The following elliptical curves are supported by the TOE

- BrainpoolP256r1 (according to [RFC 5639]),
- BrainpoolP384r1 (according to [RFC 5639]),
- BrainpoolP512r1 (according to [RFC 5639]),
- NIST P-256 (according to [RFC 5114]), and
- NIST P-384 (according to [RFC 5114]).

Alongside, the TOE supports the case of unidirectional communication with wireless meter (via the wM-Bus protocol), where the external entity is authenticated via AES with CMAC authentication. In this case, the AES algorithm is operating in CBC mode with 128-bit symmetric keys. The authentication is successful in case that the CMAC has been successfully verified by the use of a cryptographic key K_{mac}. The cryptographic key for CMAC authentication (K_{mac}) is derived from the meter individual key MK conformant to [TR-03116-3, chap. 7.2]. The meter individual key MK (brought into the TOE by the GWA) is selected by the TOE through the MAC-protected but unencrypted meter-id submitted by the meter.

The generation of the cryptographic key material for TLS secured communication channels utilizes a Security Module. This Security Module is compliant to [TR-03109-2] and evaluated according to [SecModPP].

The destruction of cryptographic key material used by the TOE is performed through "zeroisation". The TOE stores all ephemeral keys used for TLS secured communication or other cryptographic operations in the RAM only. For instance, whenever a TLS secured communication is terminated, the TOE wipes the RAM area used for the cryptographic key material with 0-bytes directly after finishing the usage of that material.

The TOE receives the authentication certificate of the external entity during the handshake phase of the TLS protocol. For the establishment of the TLS secured communication channel, the TOE verifies the correctness of the signed data transmitted during the TLS protocol handshake phase. While importing an authentication certificate the TOE verifies the certificate chain of the certificate for all certificates of the SM-PKI according to [TR-03109-4]. Note, that the certificate used for the TLS-based authentication of wired meters is self-signed and not part of the SM-PKI. Additionally, the TOE checks whether the certificate is configured by the Gateway Administrator for the used interface, and whether the remote IP address used and configured in the TSF data are identical (**FIA_USB.1**). The TOE does not check the certificate's revocation status. In order to authenticate the external entity, the key material of the TOE's communication partner must be known and trusted.

The following communication types are known to the TOE [222]:

a) WAN communication via IF_GW_WAN

[222] Please note that the TOE additionally offers the interface IF_GW_SM to the certified Security Module built into the TOE.

b) LMN communication via IF_GW_MTR (wireless or wired Meter)
c) HAN communication via IF_GW_CON, IF_GW_CLS or IF_GW_SRV

Except the communication with wireless meters at IF_GW_MTR, all communication types are TLS-based. In order to accept a TLS communication connection as being authenticated, the following conditions must be fulfilled:

a) The TLS channel must have been established successfully with the required cryptographic mechanisms.
b) The certificate of the external entity must be known and trusted through configuration by the Gateway Administrator, and associated with the according communication type[223].

For the successfully authenticated external entity, the TOE performs an internal assignment of the communication type based on the certificate received at the external interface if applicable. The user identity is associated with the name of the certificate owner in case of a certificate-based authentication or with the user name in case of a password-based authentication at interface IF_GW_CON.

For the LMN communication of the TOE with wireless (a.k.a. wM-Bus-based) meters, the external entity is authenticated by the use of the AES-CMAC algorithm and the meter-ID for wired Meters is used for association to the user identity (**FIA_USB.1**). This communication is only allowed for meters not supporting TLS-based communication scenarios.

FCS_CKM.1/TLS is fulfilled by the TOE through the implementation of the pseudorandom function of the TLS protocol compliant to [RFC 5246] while the Security Module is used by the TOE for the generation of the cryptographic key material. The use of TLS according to [RFC 5246] and the use of the postulated cipher suites according to [RFC 5639] fulfill the requirement **FCS_COP.1/TLS**. The requirements **FCS_CKM.1/MTR** and **FCS_COP.1/MTR** are fulfilled by the use of AES-CMAC-secured communication for wireless meters. The requirement **FCS_CKM.4** is fulfilled by the described method of “zeroisation” when destroying cryptographic key material. The implementation of the described mechanisms (especially the use of TLS and AES-CBC with CMAC) fulfills the requirements **FTP_ITC.1/WAN**, **FTP_ITC.1/MTR**, and

[223] Of course, this does not apply if password-based authentication is configured at IF_GW_CON.

FTP_ITC.1/USR. **FPT_RPL.1** is fulfilled by the use of the TLS protocol respectively the integration of transmission counters according to [TR-03116-3, chap. 7.3].

A successfully established connection will be automatically disconnected by the TOE if a TLS channel to the WAN is established more than 48 hours, if a TLS channel to the LMN has transmitted more than 5 MB of information or if a channel to a local user is inactive for a time configurable by the authorised Gateway Administrator of up to 10 minutes, and a new connection establishment will require a new full authentication procedure (**FIA_UAU.6**). In any case – whether the connection has been successfully established or not – all associated resources related with the connection or connection attempt are freed. The implementation of this requirement is done by means of the TOE’s operation system monitoring and limiting the resources of each process. This means that with each connection (or connection attempt) an internal session is created that is associated with resources monitored and limited by the TOE. All resources are freed even before finishing a session if the respective resource is no longer needed so that no previous information content of a resource is made available. Especially, the associated cryptographic key material is wiped as soon it is no longer needed. As such, the TOE ensures that during the phase of connection termination the internal session is also terminated and by this, all internal data (associated cryptographic key material and volatile data) is wiped by the zeroisation procedure described. Allocated physical resources are also freed. In case non-volatile data is no longer needed, the associated resources data are freed, too. The TOE doesn’t reuse any objects after deallocation of the resource (**FDP_RIP.2**).

If the external entity can be successfully authenticated on basis of the received certificate (or the password in case of a consumer using password authentication) and the acclaimed identity could be approved for the used external interface, the TOE associates the user identity, the authentication status and the connecting network to the role according to the internal role model (**FIA_ATD.1**). In order to implement this, the TOE utilizes an internal data model which supplies the allowed communication network and other restricting properties linked with the submitted security attribute on the basis of the submitted authentication data providing the multiple mechanisms for authentication of any user's claimed identity according to the necessary rules according to [TR-03109-1] (**FIA_UAU.5**).

In case of wireless meter communication (via the wM-Bus protocol), the security attribute of the Meter is the meter-id authenticated by the CMAC, where the meter-id is the identity providing criterion that is used by the TOE. The identity of the Meter is associated to the successfully authenticated external entity by the TOE and linked to the respective role according to Table 5 and its active session. In this case, the identity providing criterion is also the meter-id.

The TOE enforces an explicit and complete security policy protecting the data flow for all external entities (**FDP_IFC.2/FW**, **FDP_IFF.1/FW**, **FDP_IFC.2/MTR**, **FDP_IFF.1/MTR**). The security policy defines the accessibility of data for each external entity and additionally the permitted actions for these data. Moreover, the external entities do also underlie restrictions for the operations which can be executed with the TOE (**FDP_ACF.1**). In case that it is not possible to authenticate an external entity successfully (e.g. caused by unknown authentication credentials), no other action is allowed on behalf of this user and the concerning connection is terminated (**FIA_UAU.2**). Any communication is only possible after successful authentication and identification of the external entity (**FIA_UID.2**, **FIA_USB.1**).

The reception of the wake-up service data package is a special case that requests the TOE to establish a TLS authenticated and protected connection to the Gateway Administrator. The TOE validates the data package due to its compliance to the structure described in [TR-03109-1] and verifies the ECDSA signature with the public key of the Gateway Administrator's certificate which must be known and trusted to the TOE. The TOE does n ot perform a revocation check or any validity check compliant to the shell model. The TOE verifies the electronic signature successfully when the certificate is known, trusted and associated to the Gateway Administrator. The TOE establishes the connection to the Gateway Administrator when the package has been validated due to its structural conformity, the signature has been verified and the integrated timestamp fulfills the requirements of [TR-03109-1]. Receiving the data package and the successful validation of the wake-up package does not mean that the Gateway Administrator has successfully been authenticated.

If the Gateway Administrator could be successfully authenticated based on the certificate submitted during the TLS handshake phase, the role will be assigned by the TOE according to now approved identity based on the internal role model and the TLS channel will be established.

WAN roles

The TOE assigns the following roles in the WAN communication (**FMT_SMR.1**):

- authorised Gateway Administrator,
- authorised External Entity.

The role assignment is based on the X.509 certificate used by the external entity during TLS connection establishment. The TOE has explicit knowledge of the Gateway Administrator's certificate and the assignment of the role "Gateway Administrator" requires the successful authentication of the WAN connection.

The assignment of the role "Authorized External Entity" requires the X.509 certificate that is used during the TLS handshake to be part of an internal trust list that is under control of the TOE.

The role "Authorized External Entity" can be assigned to more than one external entity.

HAN roles

The TOE differentiates and assigns the following roles in the HAN communication (**FMT_SMR.1)**:

- authorised Consumer
- authorised Service Technician

The role assignment is based on the X.509 certificate used by the external entity for TLS-secured communication channels or on password-based authentication at interface IF_GW_CON if configured (**FIA_USB.1**).

The assignment of roles in the HAN communication requires the successful identification of the external entity as a result of a successful authentication based on the certificate used for the HAN connection. The certificates used to authenticate the "Consumer" or the "Service Technician" are explicitly known to the TOE through configuration by the Gateway Administrator.

Multi-client capability in the HAN

The HAN communication might use more than one, parallel and independent authenticated communication channels. The TOE ensures that the certificates that are used for the authentication are different from each other.

The role "Consumer" can be assigned to multiple, parallel sessions. The TOE ensures that these parallel sessions are logically distinct from each other by the use of different authentication information. This ensures that only the Meter Data associated with the authorized user are provided and Meter Data of other users are not accessible.

LMN roles

One of the following authentication mechanisms is used for Meters:

a) authentication by the use of TLS according to [RFC 5246] for wired Meters

a) authentication by the use of AES with CMAC authentication according to [RFC 3394] for wireless Meters.

The TOE explicitly knows the identification credentials needed for authentication (X.509 certificate when using TLS; meter-id in conjunction with CMAC and known K_{mac} when using AES) through configuration by the Gateway Administrator. If the Meter could be successfully authenticated and the claimed identity could thus be proved, the according role “Authorised External Entity” is assigned by the TOE for this Meter at IF_GW_MTR based on the internal role model.

LMN multi-client capabilities

The LMN communication can be run via parallel, logically distinct and separately authenticated communication channels. The TOE ensures that the authentication credentials of each separate channel are different.

The TOE’s internal policy for access to data and objects under control of the TOE is closely linked with the identity of the external entity at IF_GW_MTR according to the TOE-internal role model. Based on the successfully verified authentication data, a permission catalogue with security attributes is internally assigned, which defines the allowed actions and access permissions within a communication channel.

The encapsulation of the TOE processes run by this user is realized through the mechanisms offered by the TOE´s operating system and very restrictive user rights for each process. Each role is assigned to a separate, limited user account in the TOE´s operating system. For all of these accounts, it is only allowed to read, write or execute the files absolutely necessary for implementing the program logic. For each identity interacting with the TOE, a separate operating system process is started. Especially, the databases used by the TOE and the logging service are adequately separated for enforcement of the necessary security domain separation (**FDP_ACF.1**). The allowed actions and access permissions and associated objects are assigned to the successfully approved identity of the user based on the used authentication credentials and the resulting associated role. The current session is unambiguously associated with this user. No interaction (e.g. access to Meter Data) is possible without an appropriate permission catalogue (**FDP_ACC.2**). The freeing of the role assignment and associated resources are ensured through the monitoring of the current session.

7.2 SF.2: Acceptance and Deposition of Meter Data, Encryption of Meter Data for WAN transmission

The TOE receives Meter Data from an LMN communication channel and deposits these Meter Data with the associated data for tariffing in a database especially assigned to this individual Meter residing in an encrypted file system (**FCS_COP.1/MEM**). The time interval for receiving or retrieving Meter Data can be configured individually per meter through a successfully authenticated Gateway Administrator and are initialized by the TOE during the setup procedure with pre-defined values.

The Meter Data are cryptographically protected and their integrity is verified by the TOE before the tariffing and deposition is performed. In case of a TLS secured communication, the integrity and confidentiality of the transmitted data is protected by the TLS protocol according to [RFC 5246]. In case of a unidirectional communication at IF_GW_MTR/wireless, the integrity is verified by the verification of the CMAC check sum whereas the protection of the confidentiality is given by the use of AES in CBC mode with 128 bit key length in combination with the CMAC authentication (**FCS_CKM.1/MTR**, **FCS_COP.1/MTR**). The AES encryption key has been brought into the TOE via a management function during the pairing process for the Meter. In the TOE's internal data model, the used cryptographic keys K_{mac} and K_{enc} are associated with the meter-id due to the fact of the unidirectional communication. The TOE contains a packet monitor for Meter Data to avoid replay attacks based on the re-sending of Meter Data packages. In case of recognized data packets which have already been received and processed by the TOE, these data packets are blocked by the packet monitor (**FPT_RPL.1**).

Concerning the service layers, the TOE detects replay attacks that can occur during authentication processes against the TOE or for example receiving data from one of the involved communication networks. This is for instance achieved through the correct interpretation of the strictly increasing ordering numbers for messages from the meters (in case that a TLS-secured communication channel is not used), through the enforcement of an appropriate time slot of execution for successfully authenticated wake-up calls, and of course through the use of the internal means of the TLS protocol according to [RFC 5246] (**FPT_RPL.1**).

The deposition of Meter Data is performed in a way that these Meter Data are associated with a permission profile. This means that all of the operations and actions that can be taken with these data as described afterwards (e.g. sending via WAN to an Authenticated External Entity) depend on the permissions which are associated with the

Meter Data. For metrological purposes, the Meter Data's security attribute - if applicable - will be persisted associated with its corresponding Meter Data by the TOE. All user associated data stored by the TOE are protected by an AES-128-CMAC value. Before accessing these data, the TOE verifies the CMAC value that has been applied to the user data and detects integrity errors on any data and especially on user associated Meter Data in a reliable manner (**FDP_SDI.2**).

Closely linked with the deposition of the Meter Data is the assignment of an unambiguous and reliable timestamp on these data. The reliability grounds on the regular use of an external time source offering a sufficient exactness (**FPT_STM.1**) which is used to synchronize the operating system of the TOE. A maximum deviation of 3% of the measuring period is allowed to be in conformance with [PP_GW]. The data set (Meter Data and tariff data) is associated with the timestamp in an inseparably manner because each Meter Data entry in the database includes the corresponding time stamp and the database is cryptographically protected through the encrypted file system. For details about database encryption please see page 150).

For transmission of consumption data (tariffed Meter Data) or status data into the WAN, the TOE ensures that the data are encrypted and digitally signed (**FCO_NRO.2**, **FCS_CKM.1/CMS**, **FCS_COP.1/CMS**, **FCS_COP.1/HASH**, **FCS_COP.1/MEM**). In case of a successful transmission of consumption data into the WAN, beside the transmitted data the data's signature applied by the TOE is logged in the Consumer-Log for the respective Consumer at IF_GW_CON thus providing the possibility not only for the recipient to verify the evidence of origin for the transmitted data but to the Consumer at IF_GW_CON, too (**FCO_NRO.2**). The encryption is performed with the hybrid encryption as specified in [TR-03109-1-I] in combination with [TR-03116-3]. The public key of the external entity, the data have to be encrypted for, is known by the TOE through the authentication data configured by the Gateway Administrator and its assigned identity. This public key is assumed by the TOE to be valid because the TOE does not verify the revocation status of certificates. The public key used for the encryption of the derived symmetric key used for transmission of consumption data is different from the public key in the TLS certificate of the external entity used for the TLS secured communication channel. The derivation of the hybrid key used for transmission of consumption data is done according to [TR-03116-3, chapter 8].

The TOE does also foresee the case that the data is encrypted for an external entity that is not directly assigned to the external entity holding the active communication channel. The electronic signature is created through the utilization of the Security Module whereas the TOE is responsible for the computation of the hash value for the data to be signed. Therefore, the TOE utilizes the SHA-256 or SHA-384 hash algorithm. The SHA-512 hash algorithm is available in the TOE but not yet used (**FCS_COP.1/HASH**). The data to be sent to the external entity are prepared on basis of the tariffed meter data. The data to be transmitted are removed through deallocation of the resources after the (successful or unsuccessful) transmission attempt so that afterwards no previous information will be available (**FDP_RIP.2**). The created temporary session keys which have been used for encryption of the data are also deleted by the already described zeroisation mechanism as soon they are no longer needed (**FCS_CKM.4**).

The time interval for transmission of the data is set for a daily transmission, and can be additionally configured by the Gateway Administrator. The TOE sends randomly generated messages into the WAN, so that through this the analysis of frequency, load, size or the absence of external communication is concealed (**FPR_CON.1**). Data that are not relevant for accounting are aliased for transmission so that no personally identifiable information (PII) can be obtained by an analysis of not billing-relevant information sent to parties in the WAN. Therefore, the TOE utilizes the alias as defined by the Gateway Administrator in the Processing Profile for the Meter identity to external parties in the WAN. Thereby, the TOE determines the alias for a user and verifies that it conforms to the alias given in the Processing Profile (**FPR_PSE.1**).

7.3 SF.3: Administration, Configuration and SW Update

The TOE includes functionality that allows its administration and configuration as well as updating the TOE's complete firmware ("firmware updates") or only the software application including the service layer ("software updates"). This functionality is only provided for the authenticated Gateway Administrator (**FMT_MOF.1**, **FMT_MSA.1/AC**, **FMT_MSA.1/FW**, **FMT_MSA.1/MTR**).

The following operations can be performed by the successfully authenticated Gateway Administrator:

a) Definition and deployment of Processing Profiles including user administration, rights management and setting configuration parameters of the TOE
b) Deployment of tariff information
c) Deployment and installation of software/firmware updates

A complete overview of the possible management functions is given in Table 14 and Table 15 (**FMT_SMF.1**). Beside the possibility for a successfully authenticated Service Technician to view the system log via interface IF_GW_SRV, administrative or configuration measures on the TOE can only be taken by the successfully authenticated Gateway Administrator.

In order to perform these measures, the TOE has to establish a TLS secured channel to the Gateway Administrator and must authenticate the Gateway Administrator successfully. There are two possibilities:

a) The TOE independently contacts the Gateway Administrator at a certain time specified in advance by the Gateway Administrator.

b) Through a message sent to the wake-up service, the TOE is requested to contact the Gateway Administrator.

In the second case, the wake-up data packet is received by the TOE from the WAN and checked by the TOE for structural correctness according to [TR-03109-1]. Afterwards, the TOE verifies the correctness of the electronic signature applied to the wake-up message data packet using the certificate of the Gateway Administrator stored in the TSF data. Afterwards, a TLS connection to the Gateway Administrator is established by the TOE and the above mentioned operations can be performed.

Software/firmware updates always have to be signed by the TOE manufacturer.

Software/firmware updates can be of different content:

a) The whole boot image of the TOE is changed.

b) Only individual components of the TOE are changed. These components can be the boot loader plus the static kernel or the SMGW application.

The update packet is realized in form of an archive file enveloped into a CMS signature container according to [RFC 5652]. The electronic signature of the update packet is created using signature keys from the TOE manufacturer. The verification of this signature is performed by the TOE using the TOE's Security Module using the trust anchor of the TOE manufacturer. If the signature of the transferred data could not be successfully verified by the TOE or if the version number of the new firmware is not higher than the version number of the installed firmware, the received data is rejected by the TOE and not used for further processing. Any administrator action is entered in the System Log of the TOE. Additionally, an authorised Consumer can interact with the TOE via the interface IF_GW_CON to get the version number and the current time displayed (**FMT_MOF.1**).

The signature of the update packet is immediately verified after receipt. After successful verification of the update packet the update process is immediately performed. In each case, the Gateway Administrator gets notified by the TOE and an entry in the TOE´s system log will be written.

All parameters that can be changed by the Gateway Administrator are preset with restrictive values by the TOE. No role can specify alternative initial values to override these restrictive default values (**FMT_MSA.3/AC**, **FMT_MSA.3/FW**, **FMT_MSA.3/MTR**).

This mechanism is supported by the TOE-internal resource monitor that internally monitors existing connections, assigned roles and operations allowed at a specific time.

7.4 SF.4: Displaying Consumption Data

The TOE offers the possibility of displaying consumption data to authenticated Consumers at interface IF_GW_CON. Therefore, the TOE contains a web server that implements TLS-based communication with mutual authentication (**FTP_ITC.1/USR**). If the Consumer requests a password-based authentication from the GWA according to [TR-03109-1] and the GWA activates this authentication method for this Consumer, the TOE uses TLS authentication with server-side authentication and HTTP digest access authentication according to [RFC 7616]. In both cases, the requirement **FCO_NRO.2** is fulfilled through the use of TLS-based communication and through encryption and digital signature of the (tariffed) Meter Data to be displayed using **FCS_COP.1/HASH**.

To additionally display consumption data, a connection at interface IF_GW_CON must be established and the role “(authorised) Consumer” is assigned to the user with his used display unit by the TOE. Different Consumer can use different display units. The amount of allowed connection attempts at IF_GW_CON is set to 5. In case the amount of allowed connection attempts is reached, the TOE blocks IF_GW_CON (**FIA_AFL.1**). The display unit has to technically support the applied authentication mechanism and the HTTP protocol version 1.1 according to [RFC 2616] as communication protocol. Data is provided as HTML data stream and transferred to the display unit. In this case, further processing of the transmitted data stream is carried out by the display unit.

According to [TR-03109-1], the TOE exclusively transfers Consumer specific consumption data to the display unit. The Consumer can be identified in a clear and unambiguous manner due to the applied authentication mechanism. Moreover, the TOE ensures that exclusively the data actually assigned to the Consumer is provided at the display unit via IF_GW_CON (**FIA_USB.1**).

7.5 SF.5: Audit and Logging

The TOE generates audit data for all actions assigned in the System-Log (**FAU_GEN.1/SYS**), the Consumer-Log (**FAU_GEN.1/CON**), and the Calibration-Log (**FAU_GEN.1/CAL**) as well. On the one hand, this applies to the values measured by the Meter (Consumer-Log) and on the other hand to system data (System-Log) used by the Gateway Administrator of the TOE in order to check the TOE's current functional status. In addition, metrological entries are created in the Calibration-Log. The TOE thus distinguishes between the following log classes:

a) System-Log
b) Consumer-Log
c) Calibration-Log

The TOE audits and logs all security functions that are used. Thereby, the TOE component accomplishing this security audit functionality includes the necessary rules monitoring these audited events and through this indicating a potential violation of the enforcement of the TOE security functionality (e. g. in case of an integrity violation, replay attack or an authentication failure). If such a security breach is detected, it is shown as such in the log entry (**FAU_SAA.1/SYS**).

The System-Log can only be read by the authorized Gateway Administrator via interface IF_GW_WAN or by an authorized Service Technician via interface IF_GW_SRV (**FAU_SAR.1/SYS**). Potential security breaches are separately indicated and identified as such in the System-Log and the GWA gets informed about this potential security breach (**FAU_ARP.1/SYS**, **FDP_SDI.2**). Data of the Consumer-Log can exclusively be viewed by authenticated Consumers via interface IF_GW_CON designed to display consumption data (**FAU_SAR.1/CON**). The data included in the Calibration-Log can only be read by the authenticated Gateway Administrator via interface IF_GW_WAN (**FAU_SAR.1/CAL**).

If possible, each log entry is assigned to an identity that is known to the TOE. For audit events resulting from actions of identified users resp. roles, the TOE associates the generated log information to the identified users while generating the audit information (**FAU_GEN.2**).

Generated audit and log data are stored in a cryptographically secured storage. For this purpose, a file-based SQL database system is used securing its' data using an AES-XTS-128 encrypted file system (AES in XTS mode with 128-bit keys) according to [FIPS Pub. 197] and [NIST 800-38E]. This is achieved by using device-specific AES keys so that the secure environment can only be accessed with the associated symmetric key available. Using an appropriately limited access of this symmetric, the TOE implements the necessary rules so that it can be ensured that unauthorised modification or deletion is prohibited (**FAU_STG.2**).

Audit and log data are stored in separate locations: One location is used to store Consumer-specific log data (Consumer-Log) whereas device status data and metrological data are stored in a separate location: status data are stored in the System-Log and metrological data are stored in the Calibration-Log. Each of these logs is located in physically separate databases secured by different cryptographic keys. In case of several external meters, a separate database is created for each Meter to store the respective consumption and log data (**FAU_GEN.2**).

If the audit trail of the System-Log or the Consumer-Log is full (so that no further data can be added), the oldest entries in the audit trail are overwritten (**FAU_STG.2**, **FAU_STG.4/SYS**, **FAU_STG.4/CON**). If the Consumer-Log‘s oldest audit record must be kept because the period of billing verification (of usually 15 months) has not beeen reached, the TOE's metrological activity is paused until the oldest audit record gets deletable. Thereafter, the TOE's metrological activity is started again through an internal timer. Moreover, the mechanism for storing log entries is designed in a way that these entries are cryptographically protected against unauthorized deletion. This is especially achieved by assigning cryptographic keys to each of the individual databases for the System-Log, Consumer-Log and Calibration-Log.

If the Calibration-Log cannot store any further data, the operation of the TOE is stopped through the termination of its metering services and the TOE informs the Gateway Administrator by creating an entry in the System-Log, so that additional measures can be taken by the Gateway Administrator. Calibration-Log entries are never overwritten by the TOE (**FAU_STG.2**, **FAU_STG.4/CAL**, **FMT_MOF.1**).

The TOE anonymizes the data in a way that no conclusions about a specific person or user can be drawn from the log or recorded not billing relevant data. Stored consumption data are exclusively intended for accounting with the energy supplier. The data stored in the System-Log are used for analysis purposes concerning necessary technical analyses and possible security-related information.

7.6 SF.6: TOE Integrity Protection

The TOE makes physical tampering detectable through the TOE's sealed packaging of the device. So if an attacker opens the case, this can be physically noticed, e. g. by the Service Technician (**FPT_PHP.1**).

The TOE provides a secure boot mechanism. Beginning from the AES-128-encrypted bootloader protected by a digital signature applied by the TOE manufacturer, each subsequent step during the boot process is based on the previous step establishing a continuous forward-concatenation of cryptographical verification procedures. Thus, it is ensured that each part of the firmware, that means the operating system, the service layers and the software application in general, is tested by the TOE during initial startup. Thereby, a test of the TSF data being part of the software application is included. During this complete self-test, it is checked that the electronic system of the physical device, and all firmware components of the TOE are in authentic condition. This complete self-test can also be run at the request of the successfully authenticated Gateway Administrator via interface IF_GW_WAN or at the request of the successfully authenticated Service Technician via interface IF_GW_SRV. At the request of the successfully authenticated Consumer via interface IF_GW_CON, the TOE will only test the integrity of the Smart Metering software application including the service layers (without the operating system) and the completeness of the TSF data stored in the TOE’s database. Additionally, the TOE itself runs a complete self-test periodically at least once a month during normal operation. The integrity of TSF data stored in the TOE’s database is always tested during read access of that part of TSF data (**FPT_TST.1**). **FPT_RPL.1** is fulfilled by the use of the TLS protocol respectively the integration of transmission counters according to [TR-03116-3, chap. 7.3], and through the enforcement of an appropriate time slot of execution for successfully authenticated wake-up calls.

If an integrity violation of the TOE’s hardware or firmware is detected or if the deviation between local system time of the TOE and the reliable external time source is too large, further use of the TOE for the purpose of gathering Meter Data is not possible. Also in this case, the TOE signals the incorrect status via a suitable signal output on the case of the device, and the further use of the TOE for the purpose of gathering Meter Data is not allowed (**FPT_FLS.1**).

Basically, if an integrity violation is detected, the TOE will create an entry in the System Log to document this status for the authorised Gateway Administrator on interface IF_GW_WAN resp. for the authorised Service Technician on interface IF_GW_SRV, and will inform the Gateway Administrator on this incident (**FAU_ARP.1/SYS**, **FAU_GEN.1/SYS**, **FAU_SAR.1/SYS**, **FPT_TST.1**).

7.7 TSS Rationale

The following table shows the correspondence analysis for the described TOE security functionalities and the security functional requirements.

	SF.1	SF.2	SF.3	SF.4	SF.5	SF.6
FAU_ARP.1/SYS					X	(X)
FAU_GEN.1/SYS					X	(X)
FAU_SAA.1/SYS					X	
FAU_SAR.1/SYS					X	(X)
FAU_STG.4/SYS					X	
FAU_GEN.1/CON					X	
FAU_SAR.1/CON					X	
FAU_STG.4/CON					X	
FAU_GEN.1/CAL					X	
FAU_SAR.1/CAL					X	
FAU_STG.4/CAL					X	
FAU_GEN.2					X	

	SF.1	SF.2	SF.3	SF.4	SF.5	SF.6
FAU_STG.2					X	
FCO_NRO.2		X		X		
FCS_CKM.1/TLS	X					
FCS_COP.1/TLS	X					
FCS_CKM.1/CMS		X				
FCS_COP.1/CMS		X				
FCS_CKM.1/MTR	X	X				
FCS_COP.1/MTR	X	X				
FCS_CKM.4	X	X				
FCS_COP.1/HASH		X				
FCS_COP.1/MEM		X				
FDP_ACC.2	X					
FDP_ACF.1	X					
FDP_IFC.2/FW	X					
FDP_IFF.1/FW	X					
FDP_IFC.2/MTR	X					
FDP_IFF.1/MTR	X					
FDP_RIP.2	X	X				
FDP_SDI.2		X			X	

	SF.1	SF.2	SF.3	SF.4	SF.5	SF.6
FIA_ATD.1	X					
FIA_AFL.1				X		
FIA_UAU.2	X					
FIA_UAU.5	X					
FIA_UAU.6	X					
FIA_UID.2	X					
FIA_USB.1	X			X		
FMT_MOF.1			X		X	
FMT_SMF.1			X			
FMT_SMR.1	X					
FMT_MSA.1/AC			X			
FMT_MSA.3/AC			X			
FMT_MSA.1/FW			X			
FMT_MSA.3/FW			X			
FMT_MSA.1/MTR			X			
FMT_MSA.3/MTR			X			
FPR_CON.1		X				
FPR_PSE.1		X				
FPT_FLS.1						X

	SF.1	SF.2	SF.3	SF.4	SF.5	SF.6
FPT_RPL.1	X	X				x
FPT_STM.1		X				
FPT_TST.1						X
FPT_PHP.1						X
FTP_ITC.1/WAN	X					
FTP_ITC.1/MTR	X					
FTP_ITC.1/USR	X			X		

3104 **Table 19: Rationale for the SFR and the TOE Security Functionalities** [224]

[224] Please note that SFRs marked with “(X)” only have supporting effect on the fulfilment of the TSF.

8 List of Tables

9 List of Figures

3134 10 Appendix

3135 10.1 Mapping from English to German terms

English term	German term
billing-relevant	abrechnungsrelevant
CLS, Controllable Local System	dezentral steuerbare Verbraucher- oder Erzeugersysteme
Consumer	Anschlussnutzer; Letztverbraucher (im verbrauchenden Sinne); u.U. auch Einspeiser
Consumption Data	Verbrauchsdaten
Gateway	Kommunikationseinheit
Grid	Netz (für Strom/Gas/Wasser)
Grid Status Data	Zustandsdaten des Versorgungsnetzes
LAN, Local Area Network	Lokales Kommunikationsnetz
LMN, Local Metrological Network	Lokales Messeinrichtungsnetz
Meter	Messeinrichtung (Teil eines Messsystems)
Processing Profiles	Konfigurationsprofile
Security Module	Sicherheitsmodul (z.B. eine Smart Card)
Service Provider	Diensteanbieter
Smart Meter, Smart Metering System [225]	Intelligente, in ein Kommunikationsnetz eingebundene, elektronische Messeinrichtung (Messsystem)
TOE	EVG (**Ev**aluierungs**g**egenstand)

[225] Please note that the terms “Smart Meter” and “Smart Metering System” are used synonymously within this document.

WAN, Wide Area Network	Weitverkehrsnetz (für Kommunikation)

3136

3137 10.2 Glossary

Term	Description
Authenticity	property that an entity is what it claims to be (according to [SD_6])
Block Tariff	Tariff in which the charge is based on a series of different energy/volume rates applied to successive usage blocks of given size and supplied during a specified period. (according to [CEN])
BPL	*Broadband Over Power Lines*, a method of power line communication
CA	Certification Authority, an entity that issues digital certificates. CLS config
CDMA	*Code Division Multiple Access*
CLS config (secondary asset)	See chapter 3.2
CMS	Cryptographic Message Syntax
Confidentiality	the property that information is not made available or disclosed to unauthorised individuals, entities, or processes (according to [SD_6])
Consumer	End user of electricity, gas, water or heat (according to [CEN]). See chapter 3.1
DCP	*Data Co-Processor*; security hardware of the CPU
DLMS	Device Language Message Specification
DTBS	Data To Be Signed
EAL	Evaluation Assurance Level

Term	Description
Energy Service Provider	Organisation offering energy related services to the Consumer (according to [CEN])
ETH	Ethernet
external entity	See chapter 3.1
firmware update	See chapter 3.2
Gateway Administrator (GWA)	See chapter 3.1
Gateway config (secondary asset)	See chapter 3.2
Gateway time	See chapter 3.2
G.hn	Gigabit Home Networks
GPRS	*General Packet Radio Service*, a packet oriented mobile data service
Home Area Network (HAN)	In-house data communication network which interconnects domestic equipment and can be used for energy management purposes (adopted according to [CEN]).
Integrity	property that sensitive data has not been modified or deleted in an unauthorised and undetected manner (according to [SD_6])
IT-System	Computersystem
Local Area Network (LAN)	Data communication network, connecting a limited number of communication devices (Meters and other devices) and covering a moderately sized geographical area within the premises of the consumer. In the context of this ST, the term LAN is used as a hypernym for HAN and LMN (according to [CEN], adopted).

Term	Description
Local attacker	See chapter 3.4
LTE	*Long Term Evolution* mobile broadband communication standard
Meter config (secondary asset)	See chapter 3.2
Local Metrological Network (LMN)	In-house data communication network which interconnects metrological equipment.
Meter Data	See chapter 3.2
Meter Data Aggregator (MDA)	Entity which offers services to aggregate metering data by grid supply point on a contractual basis. NOTE: The contract is with a supplier. The aggregate is of all that supplier's consumers connected to that particular grid supply point. The aggregate may include both metered data and data estimated by reference to standard load profiles (adopted from [CEN])
Meter Data Collector (MDC)	Entity which offers services on a contractual basis to collect metering data related to a supply and provide it in an agreed format to a data aggregator (that can also be the DNO). NOTE: The contract is with a supplier or a pool. The collection may be carried out by manual or automatic means. ([CEN])
Meter Data Management System (MDMS)	System for validating, storing, processing and analysing large quantities of Meter Data. ([CEN])
Metrological Area Network	In-house data communication network which interconnects metrological equipment (i.e. Meters)
OEM	Original Equipment Manufacturer
OMS	Open Metering System

Term	Description
OCOTP	On-Chip One-time-programmable
Personally Identifiable Information (PII)	Personally Identifiable Information refers to information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.
RJ45	registered jack #45; a standardized physical network interface
RMII	Reduced Media Independent Interface
RTC	Real Time Clock
Service Technician	Human entity being responsible for diagnostic purposes.
Smart Metering System	The Smart Metering System consists of a Smart Meter Gateway and connected to one or more meters. In addition, CLS (i.e. generation plants) may be connected with the gateway for dedicated communication purposes.
SML	Smart Message Language
Tariff	Price structure (normally comprising a set of one or more rates of charge) applied to the consumption or production of a product or service provided to a Consumer (according to [CEN]).
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security protocol according to [RFC 5246]
TOE	Target of Evaluation - set of software, firmware and/or hardware possibly accompanied by guidance
TSF	TOE security functionality
UART	Universal Asynchronous Receiver Transmitter

Term	Description
WAN attacker	See chapter 3.4
WLAN	Wireless Local Area Network

11 Literature

[CC] Common Criteria for Information Technology Security Evaluation –

Part 1: Introduction and general model, April 2017, version 3.1, Revision 5, CCMB-2017-04-001, https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

Part 2: Security functional requirements, April 2017, version 3.1, Revision 5, CCMB-2017-04-002, https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf

Part 3: Security assurance requirements, April 2017, version 3.1, Revision 5, CCMB-2017-04-003, https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

[CEN] SMART METERS CO-ORDINATION GROUP (SM-CG) Item 5. M/441 first phase deliverable – Communication – Annex: Glossary (SMCG/Sec0022/DC)

[PP_GW] Protection Profile for the Gateway of a Smart Metering System (Smart Meter Gateway PP), Schutzprofil für die Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen, SMGW-PP, v.1.3, Bundesamt für Sicherheit in der Informationstechnik, 31.03.2014

[SecModPP] Protection Profile for the Security Module of a Smart Meter Gateway (Security Module PP), Schutzprofil für das Sicherheitsmodul der Kommunikationseinheit eines intelligenten Messsystems für Stoff- und Energiemengen, SecMod-PP, Version 1.0.2, Bundesamt für Sicherheit in der Informationstechnik, 18.10.2013

[SD_6] ISO/IEC JTC 1/SC 27 N7446, Standing Document 6 (SD6): Glossary of IT Security Terminology 2009-04-29, available at http://www.teletrust.de/uploads/media/ISOIEC_JTC1_SC27_IT_Security_Glossary_TeleTrusT_Documentation.pdf

[TR-02102] Technische Richtlinie BSI TR-02102, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Bundesamt für Sicherheit in der Informationstechnik, Version 2022-01

[TR-03109] Technische Richtlinie BSI TR-03109, Version 1.1, Bundesamt für Sicherheit in der Informationstechnik, 22.09.2021

[TR-03109-1] Technische Richtlinie BSI TR-03109-1, Anforderungen an die Interoperabilität der Kommunikationseinheit eines Messsystems, Version 1.1, Bundesamt für Sicherheit in der Informationstechnik, 17.09.2021

[TR-03109-1-I] Technische Richtlinie BSI TR-03109-1 Anlage I, CMS-Datenformat für die Inhaltsdatenverschlüsselung und -signatur, Version 1.0.9, Bundesamt für Sicherheit in der Informationstechnik, 18.03.2013

[TR-03109-1-VI] Technische Richtlinie BSI TR-03109-1 Anlage VI, Betriebsprozesse, Version 1.0, Bundesamt für Sicherheit in der Informationstechnik, 18.03.2013

[TR-03109-2] Technische Richtlinie BSI TR-03109-2, Smart Meter Gateway – Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls, Version 1.1, Bundesamt für Sicherheit in der Informationstechnik, 15.12.2014

[TR-03109-3] Technische Richtlinie BSI TR-03109-3, Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen, Version 1.1, Bundesamt für Sicherheit in der Informationstechnik, 17.04.2014

[TR-03109-4] Technische Richtlinie BSI TR-03109-4, Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways, Version 1.2.1, Bundesamt für Sicherheit in der Informationstechnik, 09.08.2017

[TR-03109-6] Technische Richtlinie BSI TR-03109-6, Smart Meter Gateway Administration, Version 1.0, Bundesamt für Sicherheit in der Informationstechnik, 26.11.2015

[TR-03111] Technische Richtlinie BSI TR-03111, Elliptic Curve Cryptography (ECC), Version 2.1, 01.06.2018

[TR-03116-3] Technische Richtlinie BSI TR-03116-3, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 3 - Intelligente Messsysteme, Stand 2023, Bundesamt für Sicherheit in der Informationstechnik, 06.12.2022

[AGD_Consumer] Handbuch für Verbraucher, Smart Meter Gateway, Version 4.11, 02.06.2023, Power Plus Communications AG

[AGD_Techniker] Handbuch für Service-Techniker, Smart Meter Gateway, Version 5.6, 05.07.2023, Power Plus Communications AG

[AGD_GWA] Handbuch für Hersteller von Smart-Meter Gateway-Administrations-Software, Smart Meter Gateway, Version 4.13, 01.09.2023, Power Plus Communications AG

[AGD_SEC] Auslieferungs- und Fertigungsprozeduren, Anhang Sichere Auslieferung, Version 1.4, 12.05.2021, Power Plus Communications AG

[SMGW_Logging] Logmeldungen, SMGW Version 1.3 & 2.1 & 2.1.1, Version 3.4, 11.05.2023, Power Plus Communications AG

[FIPS Pub. 140-2] NIST, FIPS 140-3, Security Requirements for cryptographic modules, 2019

[FIPS Pub. 180-4] NIST, FIPS 180-4, Secure Hash Standard, 2015

[FIPS Pub. 197] NIST, FIPS 197, Advances Encryption Standard (AES), 2001

[IEEE 1901] IEEE Std 1901-2010, IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications, 2010

[IEEE 802.3] IEEE Std 802.3-2008, IEEE Standard for Information technology, Telecommunications and information exchange between systems, Local and metropolitan area networks, Specific requirements, 2008

[ISO 10116] ISO/IEC 10116:2006, Information technology -- Security techniques -- Modes of operation for an n-bit block cipher, 2006

[NIST 800-38A] NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, December 2001, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

[NIST 800-38D] NIST Special Publication 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, M. Dworkin, November 2007, http://csrc.nist.gov/publications/nistpubs/800-38D/SP-800-38D.pdf

[NIST 800-38E] NIST Special Publication 800-38E, Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, M. Dworkin, January, 2010, http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf

[RFC 2104] RFC 2104, HMAC: Keyed-Hashing for Message Authentication, M. Bellare, R. Canetti und H. Krawczyk, February 1997, http://rfc-editor.org/rfc/rfc2104.txt

[RFC 2616] RFC 2616, Hypertext Transfer Protocol - HTTP/1.1, R. Fielding, J. Gettys, J. Mogul, H. Frystyk, P. Masinter, P. Leach, T. Berners-Lee, June 1999, http://rfc-editor.org/rfc/rfc2616.txt

[RFC 7616] RFC 7616, HTTP Digest Access Authentication, R. Shekh-Yusef, D. Ahrens, S. Bremer, September 2015, http://rfc-editor.org/rfc/rfc7616.txt

[RFC 3394] RFC 3394, Schaad, J. and R. Housley, Advanced Encryption Standard (AES) Key Wrap Algorithm, September 2002, http://rfc-editor.org/rfc/rfc3394.txt

[RFC 3565] RFC 3565, J. Schaad, Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS), July 2003, http://rfc-editor.org/rfc/rfc3565.txt

[RFC 4493] IETF RFC 4493, The AES-CMAC Algorithm, J. H. Song, J. Lee, T. Iwata, June 2006, http://www.rfc-editor.org/rfc/rfc4493.txt

[RFC 5083] RFC 5083, R. Housley, Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type, November 2007, http://www.ietf.org/rfc/rfc5083.txt

[RFC 5084] RFC 5084, R. Housley, Using AES-CCM and AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS), November 2007, http://www.ietf.org/rfc/rfc5084.txt

[RFC 5114] RFC 5114, Additional Diffie-Hellman Groups for Use with IETF Standards, M. Lepinski, S. Kent, January 2008, http://www.ietf.org/rfc/rfc5114.txt

[RFC 5246] RFC 5246, T. Dierks, E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.2, August 2008, http://www.ietf.org/rfc/rfc5246.txt

[RFC 5289] RFC 5289, TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM), E. Rescorla, RTFM, Inc., August 2008, http://www.ietf.org/rfc/rfc5289.txt

[RFC 5639] RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, M. Lochter, BSI, J. Merkle, secunet Security Networks, March 2010, http://www.ietf.org/rfc/rfc5639.txt

[RFC 5652] RFC 5652, Cryptographic Message Syntax (CMS), R. Housley, Vigil Security, September 2009, http://www.ietf.org/rfc/rfc5652.txt

[EIA RS-485] EIA Standard RS-485, Electrical Characteristics of Generators and Receivers for Use in Balanced Multipoint Systems, ANSI/TIA/EIA-485-A-98, 1983/R2003

[EN 13757-1] M-Bus DIN EN 13757-1: Kommunikationssysteme für Zähler und deren Fernablesung Teil 1: Datenaustausch

[EN 13757-3] M-Bus DIN EN 13757-3, Kommunikationssysteme für Zähler und deren Fernablesung Teil 3: Spezielle Anwendungsschicht

[EN 13757-4] M-Bus DIN EN 13757-4, Kommunikationssysteme für Zähler und deren Fernablesung Teil 4: Zählerauslesung über Funk, Fernablesung von Zählern im SRD-Band von 868 MHz bis 870 MHz

[IEC-62056-5-3-8] Electricity metering – Data exchange for meter reading, tariff and load control – Part 5-3-8: Smart Message Language SML, 2012

[IEC-62056-6-1] IEC-62056-6-1, Datenkommunikation der elektrischen Energiemessung, Teil 6-1: OBIS Object Identification System, 2017, International Electrotechnical Commission

[IEC-62056-6-2] IEC-62056-6-2, Datenkommunikation der elektrischen Energiemessung - DLMS/COSEM, Teil 6-2: COSEM Interface classes, 2017, International Electrotechnical Commission

[IEC-62056-21] IEC-62056-21, Direct local data exchange - Mode C, 2011, International Electrotechnical Commission

[LUKS] LUKS On-Disk Format Specification Version 1.2.1, Clemens Fruhwirth, October 16th, 2011

[PACE] The PACE-AA Protocol for Machine Readable Travel Documents, and its Security, Jens Bender, Ozgur Dagdelen, Marc Fischlin and Dennis Kügler, http://fc12.ifca.ai/pre-proceedings/paper_49.pdf

[X9.63] ANSI X9.63, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, 2011

[G865] DVGW-Arbeitsblatt G865 Gasabrechnung, 11/2008

[VDE4400] VDE-AR-N 4400:2011-09, Messwesen Strom, VDE-Anwendungsregel, 01.09.2011

[DIN 43863-5] DIN: Herstellerübergreifende Identifikationsnummer für Messeinrichtungen, 2012

[USB] Universal Serial Bus Specification, Revision 2.0, April 27, 2000, USB Communications CLASS Specification for Ethernet Devices, http://www.usb.org/developers/docs/usb20_docs/#usb20spec

[ITU G.hn] G.996x Unified high-speed wireline-based home networking transceivers, 2018

Power Plus Communications AG
Dudenstraße 6, 68167 Mannheim
Tel. 00 49 621 40165 100 | Fax. 00 49 621 40165 111
info@ppc-ag.de | www.ppc-ag.de