Dr. Neuhaus

SMARTY IQ-SMGW LTE Security Target

Author: Sagemcom Dr. Neuhaus GmbH

Version: 1.31
Date: 28.09.2022

Abstract
This document is the Security Target (ST) for the Common Criteria certification of SMARTY IQ-SMGW LTE Version 1.1

Keywords
Smart Meter System,Gateway,Common Criteria,Smart Meter Gateway ASE

This page intentionally left blank

Table of content

List of Tables

List of Figures

1 ST introduction

1.1 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]).

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 consumer's 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.

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). The security functionality of the TOE comprises

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

mainly to protect the privacy of consumers, to ensure a reliable billing process and to protect the Smart Metering System and a corresponding large scale infrastructure of the smart grid. The availability of the Gateway is not addressed by this ST

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

[2] Please note that such functionality requires 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.

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

1.2 ST Reference

Title	SMARTY IQ-SMGW LTE Security Target
Version	1.31
Date	28.09.2022
Authors	Sagemcom Dr. Neuhaus GmbH
Certification Authority	Bundesamt für Sicherheit in der Informationstechnik (BSI) Federal Office for Information Security, Germany
Certification-ID	BSI-DSZ-CC-0822
Evaluation Assurance Level	EAL 4 augmented by AVA_VAN.5 and ALC_FLR.2
CC-Version	3.1 Revision 4
Keywords	Smart Metering, Security Target, Meter, Gateway, ST
PP Conformance	This ST claims strict conformance to [SMGW-PP].

1.3 TOE Reference

The TOE is uniquely identified as follows:

TOE Identification	**SMARTY IQ-SMGW LTE**[5]
TOE Version	Version 1.1
TOE Parts	Hardware Version: DNT8209/3.3 Software Version: 2.0.3036 Operating System Version: DNT8209-21
TOE Developer	Sagemcom Dr. Neuhaus GmbH
TOE Type	Smart Meter Gateway according to [SMGW-PP]
TOE Definition	Device consisting of a hardware and software The Security Module according to [SM-PP] is not part of the TOE.

The following table list the public manuals the customer will get with the TOE.

document title	**Anleitung zur IT-Sicherheit / Guidance Document – Anleitung zum Betrieb**
file	Dr. Neuhaus Smarty IQ AGD_OPE_128.pdf
hash sha256	ea9ad5588bb0058c848e7ef7476240fb87cc47022787e79451026591cbc676b2
document title	**Anleitung zur IT-Sicherheit / Guidance Document – Vorbereitende Maßnahmen**
file	Dr. Neuhaus Smarty IQ AGD_PRE_126.pdf
hash sha256	884e60f5b944f05a4332e3ca1d75f3a7cd4102f3c65c255b539c96b5f7202846
document title	**Sichere Lieferkette**
file	Gateway_Dr.Neuhaus_ALC_SichereLieferkette_1.3.pdf
hash sha256	3ad99a0fa18b7918821ac70255a031d4b0d88c64ea57cd22402748be8b21b375
document title	**Anlage zum AGD: Dr. Neuhaus Spezifikation SMGW - Http Gateway Protocol, Version 2.4**

[5] Die Bezeichnungen SMARTY IQ-LTE und SMARTY IQ-SMGW LTE werden synonym verwendet.

file	HGP-DatenModell 2.4.026.pdf
hash sha256	7448a50402a3c47331429e932353575b72fedb2743e928dd2fc8eed1ef8c3049
document title	**Anlage zum AGD: Auszug aus der Funktionalen Spezifikation mit der Übersicht der Audit Records**
file	FSP_1.37-AuditRecords.pdf
hash sha256	c99697f8e87cc93d3c74607de72b110c8691872b066cd8e5c5c9ec5d052bb439
document title	**Anlage zum AGD: Auszug aus der Funktionalen Spezifikation mit der Übersicht der versendeten Events**
file	FSP_1.37-Events.pdf
hash sha256	dc4db45ea26695784682b47edda59edcab5bf506df1718ef63ac53b34f748339

Table 1: Public TOE documents

1.4 Specific terms

Various different vocabularies exist in the area of Smart Grid, Smart Metering, and Home Automation. Further, the Common Criteria maintain their own vocabulary. The following table provides an overview over the most prominent terms that are used in this Protection Profile and should serve to avoid any bias. A complete glossary and list of acronyms can be found in chapter 8.2.

Term	Definition	Source (if any)
CLS, Controllable Local Systems	CLS are systems containing IT-components in the Home Area Network (HAN) of the consumer that do not belong to the Smart Metering System but may use the Gateway for dedicated communication purposes. CLS may range from local power generation plants, controllable loads such as air condition and intelligent household appliances (“white goods”) to applications in home automation.	
Commodity	Electricity, gas, water or heat[6]	
Consumer	End user of electricity, gas, water or heat. The consumer can also generate energy using a Distributed Energy Resource.	[CEN]
Gateway Smart Meter Gateway (SMGW)[7]	Device or unit responsible for collecting Meter Data, processing Meter Data, providing communication capabilities for devices in the LMN, protecting devices in the LAN (such as Controllable Local Systems) against attacks from the WAN and providing cryptographic primitives (in cooperation with a Security Module). The Gateway is specified in this document and combines aspects of the following devices according to [CEN]: Meter Data Collector Meter Data Management System Meter Data Aggregator The Gateway does not aim to be a complete implementation of those devices but focuses on the required security functionality.	
Gateway Administrator	Authority that installs, configures, monitors, and controls the Smart Meter Gateway.	
HAN, Home Area Network	In-house data communication network which interconnects domestic equipment and can be used for energy management purposes.	[CEN], adopted
LAN, Local Area Network	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 PP the term LAN is used as a hypernym for HAN and LMN.	[CEN], adopted
LMN, Local Metrological Network	In-house data communication network which interconnects metrological equipment.	
Meter	The term Meter refers to a unit for measuring the consumption or production of a certain commodity with additional functionality. It collects consumption or production data and transmits this data to the Gateway. As not all aspects of a Smart Meter according to [CEN] are implemented in the descriptions within this document the term Meter is used. The Meter has to be able to encrypt and sign the data it sends and will typically deploy a Security Module for this. Please note that the term Meter refers to metering devices for all	[CEN], adopted

[6] Please note that this list does not claim to be complete.

[7] Please note that the terms “Gateway” and “Smart Meter Gateway” (SMGW) are used synonymously within this document

Term	Definition	Source (if any)
	kinds of commodities.	
Meter Data	Meter readings that allow calculation of the quantity of a commodity, for example electricity, gas, water or heat consumed or produced over a period. Other readings and data may also be included[8] (such as quality data, events and alarms).	[CEN]
Security Module	A Security device utilised by the Gateway for cryptographic support – typically realised in form of a smart card. The complete description of the Security Module can be found in [SM-PP].	
Service Technician	Human entity that is 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.	
User, external entity	Human or IT entity possibly interacting with the TOE from outside of the TOE boundary.	[CC]
WAN, Wide Area Network	Extended data communication network connecting a large number of communication devices over a large geographical area.	[CEN]

Table 2: Specific Terms

[8] Please note that these readings and data may require an explicit endorsement of the consumer

1.5 TOE Overview

1.5.1 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.

1.5.2 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.[9]

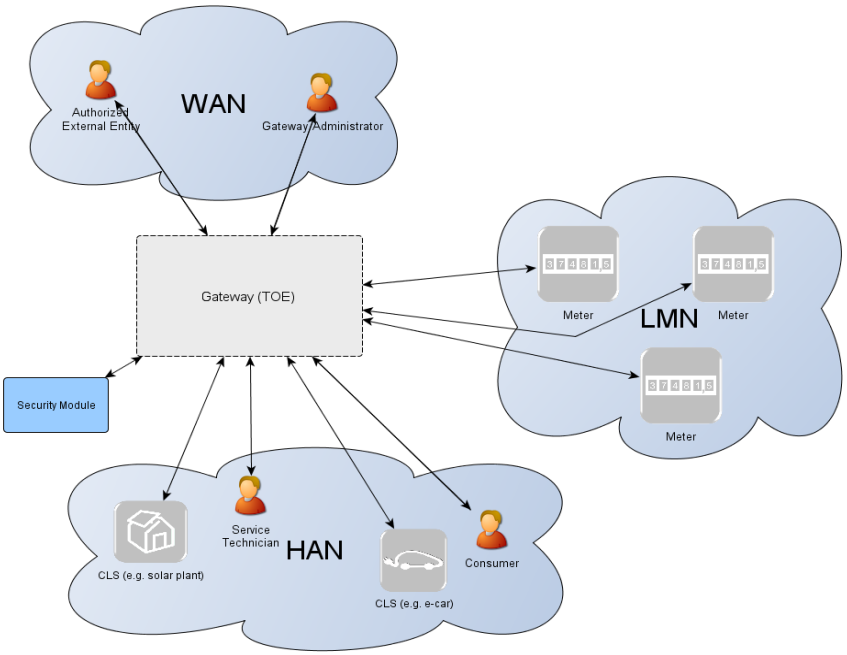

Figure 1: The TOE and its direct environment

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 LAN of the consumer (such as meters and added generation plants) 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 from Meter(s) and ensures that only authorised parties have access to them or derivatives thereof. Before sending Meter Data[10] 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 confidentiali-

[9] 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.

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

ty, authenticity, and integrity. The Meter is comparable to a classical meter[11] 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[12].

- 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. [SM-PP]).

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, the following chapters of this ST will place dedicated requirements on the way an information flow can be initiated[13].

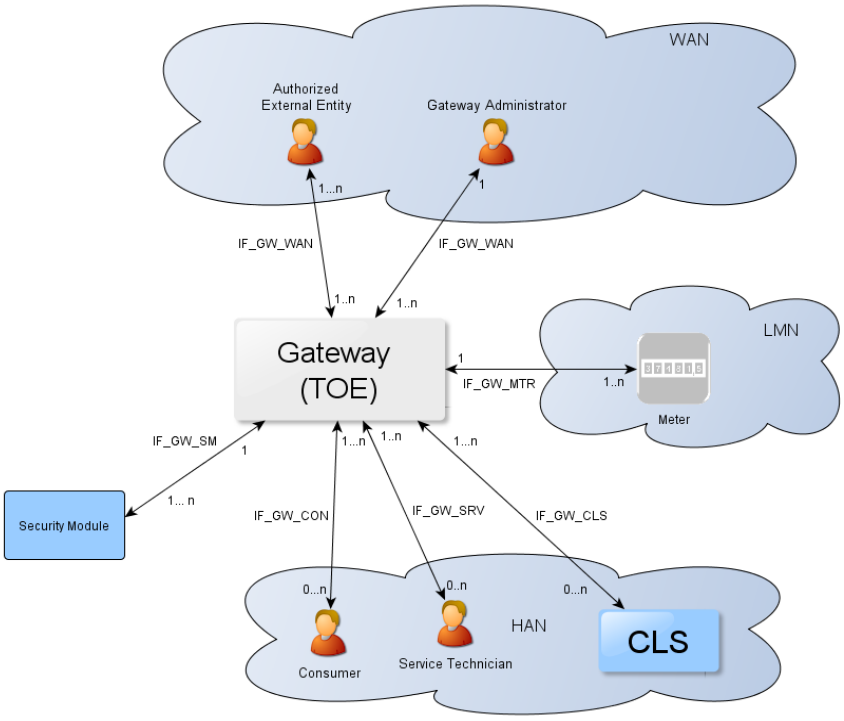

Figure 2: The logical interfaces of the TOE

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

[12] 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.

[13] 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.

The overview of the Smart Metering System as described before is based on a thread model that has been developed for Smart Metering System and has been motivated by the following considerations:

- The Gateway is the central communication unit in the Smart Metering System. It shall be 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 collect, processes and stores Meter Data. It therewith is the primary point for user interaction in the context of the Smart Metering System.
- 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.

1.5.3 Requirements on the operational environment of the TOE

The TOE shall be installed in a non-public environment within the premises of the consumer that provides a basic level of physical protection.

1.5.4 TOE description

The Smart Meter 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[14] 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 Gateway are introduced in chapter 3.1.

The TOE has a fail-safe design that specifically ensures that any malfunction cannot impact the delivery of a commodity, e.g. energy, gas or water[15].

[14] 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.

[15] Indeed, this Protection Profile 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 Protection Profile. 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.

1.5.5 TOE type

The TOE is a communication Gateway. It provides different external communication interfaces and enables the data communication between these interfaces and connected IT systems. It further collects, processes, and stores Meter Data.

1.5.6 TOE physical boundary

The TOE comprises the hardware, the software and the operating system accompanied by its guidance documentation.

The hardware and software parts of the TOE are described in the following subsections.

1.5.6.1 Overview of the TOE hardware

The following Figure 3 provides an overview about the casing and the external interfaces of the TOE.

Figure 3: SMARTY IQ-SMGW LTE casing and external interfaces

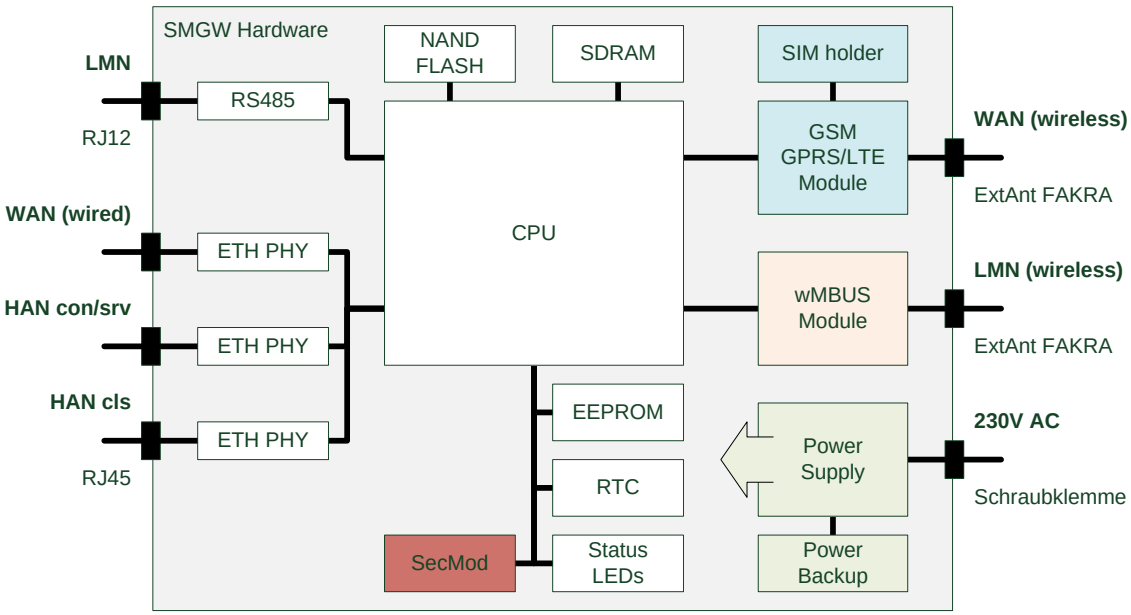

Figure 4: SMARTY IQ-SMGW LTE internal structure

The hardware consists of the following components as shown in Figure 4:

Power supply The Power supply provides the required voltages. A power reserve is maintained for a power loss in order to take through a normal shutdown without data loss.

CPU the Processor

SDRAM The RAM is used by the CPU as main storage.

NAND Flash The Flash–Memory is used as a persistent Storage.

EEPROM The EEPROM is used as a persistent Storage for hardware-parameters like Ethernet-addresses or hardware-id which will required by the boot process.

Status–LEDs The LEDs are used to indicate the Status of the SMGW e.g. Power, TLS connected, LMN data.

Security Module The Security Module is integrated into SMARTY IQ-SMGW LTE but is not part of the TOE. Mainly the TOE uses the functionality of the Security Module for cryptographic support. For more information please refer to subsection 1.5.9.

LTE module with SIM-Card Holder
The LTE module is used for the WAN access (IF_GW_WAN) via mobile radio technologies.

3 x **RJ45** Ethernet bush
The Ethernet is used for wired access for local users (IF_GW_SRV, IF_GW_CLS) or remote users (IF_GW_WAN).

wM-Bus Module The wM-Bus Module is used for wireless meters in the LMN-network (IF_GW_MTR).

RJ12 RS485 bush The serial RS485 is used for wired meters in the LMN-Network (IF_GW_MTR).

Clips for 230V~Power and antennas

1.5.6.2 Overview of the TOE software

The software is constructed with components as shown on Figure 5.

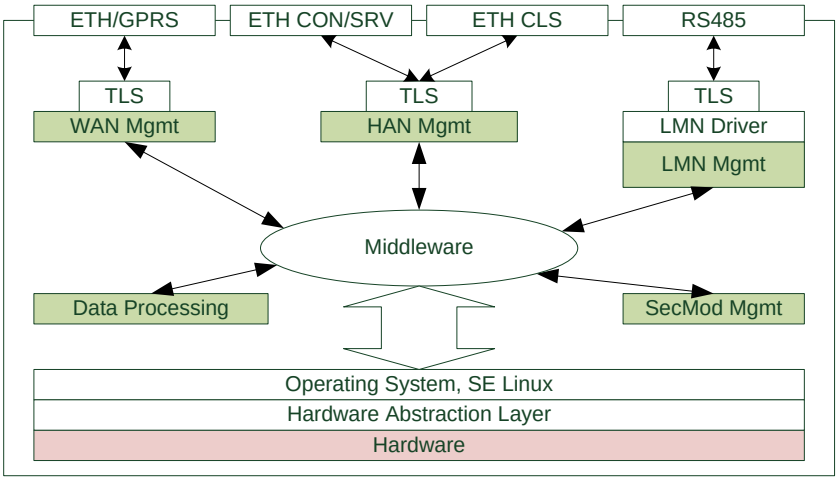

Figure 5: SMARTY IQ-SMGW LTE Overview Software components

The components will communicate rule-based via middleware. Outgoing connections are always secured with TLS.

The Subsystem WAN Mgmt contains the Admin-Connection to the GWA. The Subsystem HAN Mgmt processes all local HAN-Connections (Consumer, Service-Technician, local controls). The LMN-Interface is served by the Subsystem LMN Mgmt and its drivers. All components have access to the functions of the Security Module via middleware.

The operating system is used to separate the processes und to persistent data to files. The SE Linux Extension separates the system into logical subsystems. Only permissible access will be take place.

The Hardware Abstraction Layer is used for accessing the physical hardware.

1.5.7 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.

1.5.7.1 Handling of Meter Data[16]

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.

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 [BSI-TR-03109-1].

Please note that it is possible that a TOE enforces more than one Processing Profile, specifically if the communication and the contractual requirement for multiple external entities have to be handled.

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

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

16 Please refer to chapter 3.2 for an exact definition of the various data types.

The Gateway shall accept 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 shall maintain a calibration log with all relevant events that could affect the calibration of the Gateway.

These functionalities shall

- 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[17],
- 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[18],
- 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 (e.g. by using SSL/TLS) and ensures that consumers only get access to their own data. Please note that accessing of this interface by the consumer may happen via different technologies as long as the security requirements are fulfilled. The interface IF_GW_CON may be used by a remote display dedicated to this purpose or may be accessed by standard technologies (e.g. via a PC-based web browser)[19].

1.5.7.2 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 shall protect the privacy of the consumer and shall 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).

---

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

[18] This statement refers to the standard case and ignores that a consumer may also have an interest to manipulate the Meter Data.

[19] Please note that the access to the Gateway via a device (e.g. a laptop) that is connected to the WAN may incur a scenario for data leakage if that device is not adequately protected. The Technical Guideline [BSI-TR-03109] therefore may pose additional requirements on the way the consumer can access this interface.

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

1.5.7.3 Integrity and Authenticity protection

The Gateway shall provide the following authenticity and integrity protection:

- Verification of authenticity and integrity when receiving Meter Data from a Meter via the LMN, to verify that the Meter Data have been sent from an authentic Meter and have not been altered during transmission. 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 shall:

- prevent within the Smart Metering System that data may be sent by a non-authentic component without the possibility that the data recipient can detect this,
- facilitate the integrity of 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.

1.5.7.4 Information flow control and firewall

The Gateway shall separate devices in the LAN of the consumer from the WAN and shall enforce 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[20]; 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,

[20] 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.

- only cryptographically-protected (i.e. encrypted, integrity protected and mutually authenticated) connections are possible.[21]

These functionalities shall:

- 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 Meter Data (with the aim to cause damage to the Smart Grid), and by preventing that widely distributed Smart Metering Systems can be abused as a platform for malicious software to attack other systems in the WAN (e.g. a 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[22]:

	Source		
Destination	**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[23]	No connection establishment allowed	- (see following list)

Table 3: 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 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.

[21] 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.

[22] 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.

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

Finally, the Gateway itself shall offer the following services within the various networks:

1. The Gateway shall accept the submission of Meter Data from the LMN,
2. the Gateway shall offer a wake-up service at the WAN side as described in chapter 1.5.7.5,
3. the Gateway shall offer a user interface to the HAN that allows CLS or consumers[24] to connect to the Gateway in order to read relevant information.

1.5.7.5 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)[25].

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 [BSI-TR-03109-3] for more details) and to offer a so called wake-up service.

The Gateway shall be 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
   a) a check if the header identification is correct,
   b) the recipient is the Gateway,
   c) the wake-up packet has been sent/received within an acceptable period of time in order to prevent replayed messages,
   d) 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 shall use 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 [BSI-TR-03109-1, “Wake-Up-Service”].

[24] Please note that [BSI-TR-03109] may pose additional requirements on the interaction with the Gateway in this context.

[25] 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.

1.5.7.6 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 shall provide the consumer with transparent information about the information flows that happen with their data. In order to achieve this, the TOE shall implement a consumer log that specifically contains the information about the information flows which have 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 shall 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 shall be included in this log:

Monitoring of Data Transfers

The TOE shall be able to keep track of each data transmission in the consumer log and allow 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 shall provide 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 shall contain the parameters of each Processing Profile. The consumer log shall contain the configured addresses for internal and external entities including the CLS.

Audit Log and Monitoring

The TOE shall provide all audit data from the consumer log at the user interface IF_GW_CON. Access to the consumer log shall only be 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).

1.5.7.7 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. This Security Target defines a minimum set of management functions that must be implemented by each Gateway seeking conformance to this ST.

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.

The TOE shall provide 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.

1.5.7.8 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.

1.5.8 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[26] 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.[27]
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 read access to the system log only via this interface. He has also the possibility to view non-TSF data via this interface.

Table 4: Mandatory TOE external interfaces

1.5.9 The cryptography of the TOE and its Security Module

Parts of the cryptographic functionality used in the upper mentioned functions shall be provided by a Security Module. The Security Module provides strong cryptographic functionality, random number generation, secure storage of secrets and supports the authentication of the 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 [SM-PP]).

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

Aspect	TOE	Security Module

[26] Please note that this interface allows consumer (or consumer's CLS) to connect to the Gateway in order to read consumer specific information.

[27] 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.

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
Communication with 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 5: Cryptographic support of the TOE and its Security Module

The distribution of cryptographic functionality among the TOE and its Security Module has not only been decided from a security perspective but also considered aspects of performance. A significant part of the complex functionality is implemented by the Gateway. A state of the art Security Module in form of a smart card should be able to perform approx. 10 connection establishments per minute. As the calculated session keys are valid for a longer period this should be sufficient for most of the applications. In cases where this speed is not sufficient the developer should consider alternative approaches, e.g. the use of multiple Security Modules.

1.5.9.1 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 [BSI-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 entity 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 6:

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 [BSI-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 [BSI-TR-03109-1-I]) for the final recipient of the data[28].
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.
8. The processed Meter Data is finally submitted to an authorised external entity in the WAN via an encrypted and mutually authenticated channel.

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

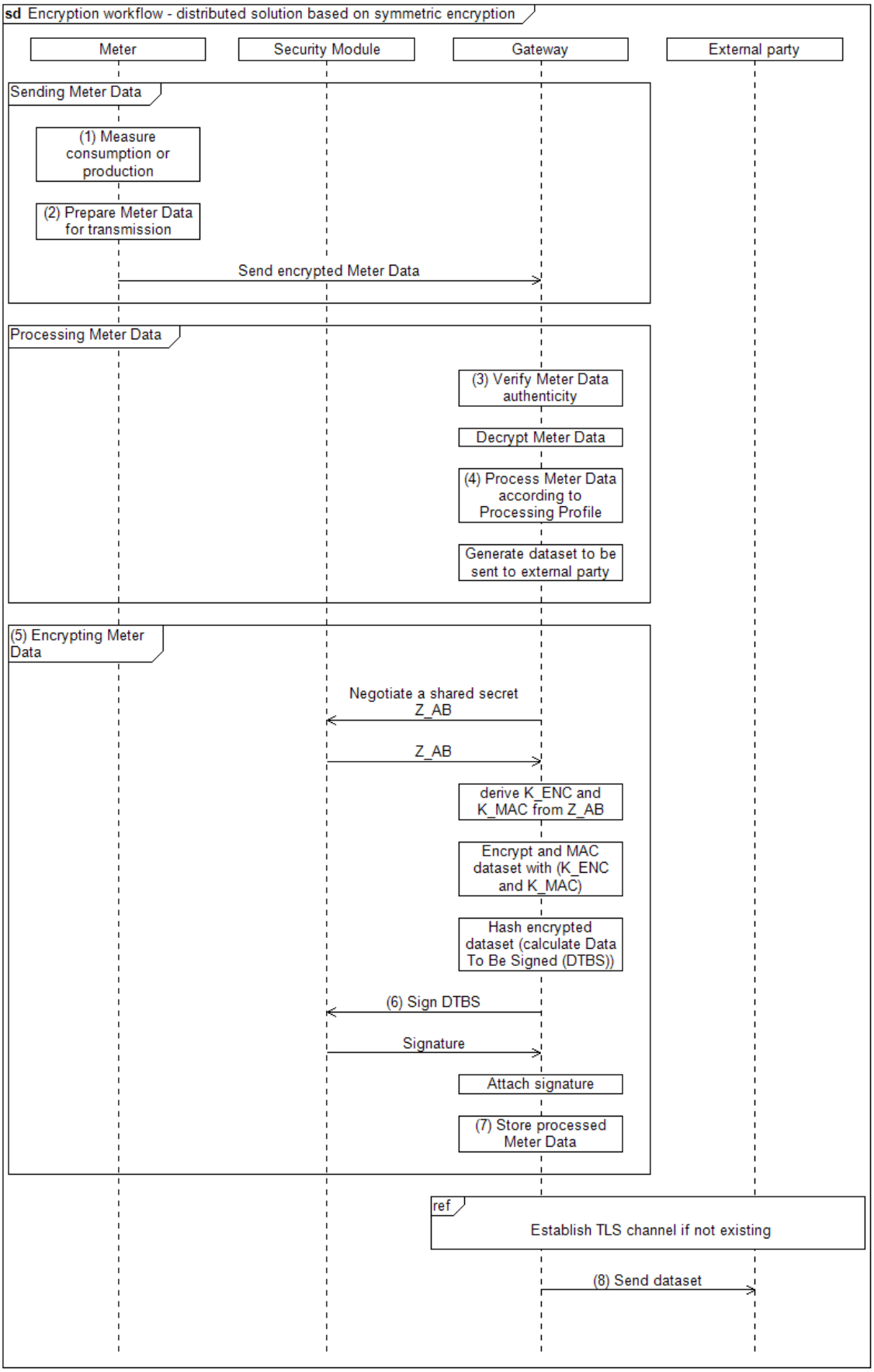

Figure 6: Cryptographic workflow for Meter, Gateway and the Security Module

1.5.10 TOE life-cycle

The life-cycle of the Gateway 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 different phases is provided in [BSI-TR-03109-1-VI].

The certified configurations of the TOE will be established after phase “Personalization”. It is ensured that previous phases are performed by trusted personal in secure environments.

2 Conformance Claims

2.1 CC Conformance Claims

This ST has been developed using Version 3.1 Revision 4 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

This ST claims strict conformance to the Common Criteria Protection Profile for the Gateway of a Smart Metering System [SMGW-PP].

2.3 Conformance claim rationale

This ST claims strict conformance only to one PP, the Gateway PP [SMGW-PP].

The security problem definition (SPD) of this ST complies with the security problem definition in the Gateway PP [SMGW-PP], as this security target claims strict conformance to the Gateway PP and no other threats, assumptions and organisational security policies are added.

The security objectives of this ST comply with the security objectives in the Gateway PP [SMGW-PP], as this security target claims strict conformance to the Gateway PP and no other security objectives are added.

The security requirements of this ST comply with the security requirements in the Gateway PP [SMGW-PP], as this security target claimed strict conformance to the Gateway PP. All assignments and selections of the security functional requirements are done in the Gateway PP [SMGW-PP] and in this security target section 6 (Security Requirements).

2.4 Package Claim

This ST conforms to assurance package EAL4 augmented by AVA_VAN.5 and ALC_FLR.2 as defined in [CC] Part 3 for product certification.

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 Protection Profile. 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).
CLS	Users by role of CLS are authorized to connect devices of Controllable Local System to the Smart Meter Gateway. Users by this role are bound to their specific Authorised External Entity.
Meter	This entity will be defined by its lmn profile and connect LMN devices to the Smart Meter Gateway. Entities by role of Meter are bound to a specific Consumer and an Authorised External Entity.
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 6: Roles used in the Protection profile

3.2 Assets

The following tables introduce the relevant assets for this Protection Profile. The tables focus on the assets that are relevant for the Gateway and do not claim to provide an overview over all assets in the Smart Metering System or for other devices in the LMN.

The following Table 7 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	• Integrity • Confidentiality (only authorised

Asset	Description	Need for Protection
	• calibration log.	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[29].	• 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 a 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

Table 7: Assets (User data)

Table 8 lists all assets typified as “TSF data”:

[29] 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

Table 8: Assets (TSF data)

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 Protection Profile 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[30],
- 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 the [BSI-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.

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.

The implementation can be found in chap. 7.7.

[30] 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.

3.4 Threats

The following sections identify the threats that are posed against the assets handled by the Smart Meter Gateway. 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 the 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 (e.g. 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 (OSPs)

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 [SM-PP] 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 [BSI-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 IF_GW_WAN of the TOE and an authorised Service Technician via IF_GW_SRV.
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 de-vices 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 5 Figure 4 shows an overview of the physical interface and its separation.

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[31].

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[32],
- 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

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

[32] 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 Protection Profile only has a limited possibility to secure this communication as both sides have to sign responsible for the quality of a cryptographic connection.

- 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 retry to send the data until a configurable number of unsuccessful retries has been reached,
- the TOE shall pseudonymise 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[33].

In addition the TOE shall generate the required keys utilising the services of its Security Module[34] , ensure that the keys are only used for an acceptable amount of time and destroy ephemeral[35] keys if not longer needed.

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

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

Specifically, the TOE shall

- 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[35],
- 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)[36],
- 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.

---

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

[34] Please refer to chapter 1.5.9 for an overview on how the cryptographic functions are distributed between the TOE and its Security Module.

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

[36] 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 Protection Profile. 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 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 and that only authentic and integrity protected updates are applied.

O.Log The TOE shall maintain a set of log files as defined in [BSI-TR-03109-1] 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 an accumulation 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 al-lowed 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 in-voice) 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[37]. Access control shall depend on the destination interface that is used to send that information.

[37] 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.

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 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 [SM-PP] 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 Protection Profile 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 [BSI-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 Objectives 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.PhysicalProtection	OE.Profile	OE.Update	OE.Network	OE.Keygen
T.DataModificationLocal				X	X		X	X					X	X				
T.DataModificationWAN	X				X		X	X					X					
T.TimeModification					X	X	X	X					X	X				
T.DisclosureWAN	X		X		X		X	X					X					
T.DisclosureLocal				X	X		X	X					X	X				
T.Infrastructure	X	X		X	X		X	X					X					
T.ResidualData							X	X					X					
T.ResidentData	X				X		X	X		X			X	X				
T.Privacy	X		X	X	X		X	X					X		X			
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 9: 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** 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 Me-

ter. **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 entities 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

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 PP:

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 10: List of Security Functional Requirements

6.2 Class FAU: Security Audit

6.2.1 Introduction

A 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 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
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) • Billing-relevant data needed to verify an invoice	• Calibration relevant data only
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 11: 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 [none]*[38]] 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] level of audit; and

c) [*none*][39]**.**

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, [*information about component triggering the event, event-relevant data*][40].

Hierarchical to: No other components

Dependencies: FPT_STM.1

The following Table 12 shows the auditable actions per SFR and the assignment to the system or consumer log.

Class FAU: Security Audit		Log
FAU_ARP.1/SYS	Minimal: Actions taken due to potential security violations.	SYS
FAU_GEN.1/SYS	-	
FAU_SAA.1/SYS	Minimal: Enabling and disabling of any of the analysis mechanisms; Minimal: Automated responses performed by the tool.	SYS
FAU_SAR.1/SYS	Basic: Reading of information from the audit records.	SYS
FAU_STG.4/SYS	Basic: Actions taken due to the audit storage failure.	SYS
FAU_GEN.1/CON	-	
FAU_SAR.1/CON	Basic: Reading of information from the audit records.	SYS
FAU_STG.4/CON	Basic: Actions taken due to the audit storage failure.	SYS
FAU_GEN.1/CAL	-	
FAU_SAR.1/CAL	Basic: Reading of information from the audit records.	SYS
FAU_STG.4/CAL	Basic: Actions taken due to the audit storage failure.	SYS, CON
FAU_GEN.2	-	
FAU_STG.2	-	

[38] PP: [assignment: list of actions]

[39] PP: [assignment: other non-privacy relevant auditable events]

[40] PP: [assignment: other audit relevant information]

Class FCO: Communication		**Log**
FCO_NRO.2	Minimal: The **failure of** invocation of the non-repudiation service Basic: Identification of the information, the destination, and a copy of the evidence provided. Refinement reason: It is not possible to store every successful generation of evidence of origin due to memory restrictions.	SYS,CON
Class FCS: Cryptographic Support		**Log**
FCS_CKM.1/TLS	Minimal: Success and failure of the activity. Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).	SYS SYS
FCS_COP.1/TLS	Minimal: Success and failure, and the type of cryptographic operation. Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.	SYS SYS
FCS_CKM.1/CMS	Minimal: ~~**Success and f**~~**F**ailure of the activity. ~~**Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).**~~ Refinement reason: It is not possible to store every successful key generation for CMS encryption due to memory restrictions. The attributes and values of CMS encryption are not configurable and static (AES-128-GCM). It´s not necessary to log every time the same value.	SYS
FCS_COP.1/CMS	Minimal: Success and failure, and the type of cryptographic operation. Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.	SYS SYS
FCS_CKM.1/MTR	Minimal: Success and failure of the activity. Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).	SYS SYS
FCS_COP.1/MTR	Minimal: Success and failure, and the type of cryptographic operation. Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.	SYS SYS
FCS_CKM.4	Minimal: Success ~~**and failure**~~ of the activity. ~~**Basic: The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys)..**~~ Refinement reason: If the Toe is unable to destroy the key (memory operation), the Toe is already out of order. Keep concealing about further details of the keys.	SYS
FCS_COP.1/HASH	Minimal: Success and failure, and the type of cryptographic operation. Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.	SYS SYS
FCS_COP.1/MEM	Minimal: Success and failure, and the type of cryptographic operation. Basic: Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.	SYS SYS
Class FDP: User Data Protection		**Log**
FDP_ACC.2	-	
FDP_ACF.1	Minimal: Successful requests to perform an operation on an object covered by the SFP. Basic: All requests to perform an operation on an object covered by the SFP.	SYS SYS
FDP_IFC.2/FW	-	
FDP_IFF.1/FW	Minimal: Decisions to permit requested information flows. Basic: All decisions on requests for information flow.	SYS SYS
FDP_IFC.2/MTR	-	
FDP_IFF.1/MTR	Minimal: Decisions to permit requested information flows. Basic: All decisions on requests for information flow.	SYS,CON, CAL SYS

FDP_RIP.2	-	
FDP_SDI.2	Minimal: failure to check the integrity of user data, including an indication of the results of the check. ~~**Basic: All attempts to check the integrity of user data, including an indication of the results of the check, if performed.**~~ **Basic: failure to check the integrity of user data, including an indication of the results of the check.** Refinement reason: It is not possible to store all successful readings due to memory restrictions.	SYS SYS
Class FIA: Identification and Authentication		**Log**
FIA_ATD.1	-	
FIA_AFL.1	Minimal: the reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).	SYS
FIA_UAU.2	Minimal: Unsuccessful use of the authentication mechanism; Basic: All use of the authentication mechanism.	SYS
FIA_UAU.5	Minimal: The final decision on authentication Basic: The result of each activated mechanism together with the final decision	SYS SYS
FIA_UAU.6	Minimal: Failure of re-authentication; Basic: All re-authentication attempts.	SYS SYS
FIA_UID.2	Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided; Basic: All use of the user identification mechanism, including the user identity provided.	SYS SYS
FIA_USB.1	Minimal: Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject). Basic: Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).	SYS
Class FMT: Security Management		**Log**
FMT_MOF.1	Basic: All modifications in the behaviour of the functions in the TSF.	SYS, CON
FMT_SMF.1	Minimal: Use of the management functions.	SYS
FMT_SMR.1	Minimal: modifications to the group of users that are part of a role;	SYS
FMT_MSA.1/AC	Basic: All modifications of the values of security attributes.	SYS
FMT_MSA.3/AC	Basic: Modifications of the default setting of permissive or restrictive rules. Basic: All modifications of the initial values of security attributes.	SYS SYS
FMT_MSA.1/FW	Basic: All modifications of the values of security attributes.	SYS
FMT_MSA.3/FW	Basic: Modifications of the default setting of permissive or restrictive rules. Basic: All modifications of the initial values of security attributes.	SYS SYS
FMT_MSA.1/MTR	Basic: All modifications of the values of security attributes.	SYS
FMT_MSA.3/MTR	Basic: Modifications of the default setting of permissive or restrictive rules. Basic: All modifications of the initial values of security attributes.	SYS
Class FPR: Privacy		**Log**
FPR_CON.1	-	
FPR_PSE.1	Minimal: The subject/user that requested resolution of the user identity should be audited.	SYS
Class FPT: Protection of the TSF		**Log**
FPT_FLS.1	Basic: Failure of the TSF.	SYS
FPT_RPL.1	Basic: Detected replay attacks.	SYS

FPT_STM.1	Minimal: changes to the time	SYS
FPT_TST.1	Basic: Execution of the TSF self tests and the results of the tests.	SYS
FPT_PHP.1	Minimal: if detection by IT means, detection of intrusion.	SYS
Class FTP: Trusted path/channels		**Log**
FTP_ITC.1/WAN	Minimal: Failure of the trusted channel functions. Minimal: Identification of the initiator and target of failed trusted channel functions. Basic: All attempted uses of the trusted channel functions. Basic: Identification of the initiator and target of all trusted channel functions.	SYS
FTP_ITC.1/MTR	Minimal: Failure of the trusted channel functions. Minimal: Identification of the initiator and target of failed trusted channel functions. Basic: All attempted uses of the trusted channel functions. Basic: Identification of the initiator and target of all trusted channel functions.	SYS
FTP_ITC.1/USR	Minimal: Failure of the trusted channel functions. Minimal: Identification of the initiator and target of failed trusted channel functions. Basic: All attempted uses of the trusted channel functions. Basic: Identification of the initiator and target of all trusted channel functions.	SYS

Table 12: Auditable Actions per SFR

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 [*all Monitoring-Events in Table 13*][41] known to indicate a potential security violation;

b) [
- Push Error (Meter Data not confirmed by the receiving EMT)
- first successful Push after an error occurs (Meter Data confirmed by the receiving EMT)
][42].

Hierarchical to: No other components

Dependencies: FAU_GEN.1

The following Table 13 shows the rules for the audit analyser and the derived actions in the system. Audits which trigger no action are normal audits for logging the normal functions auf the system.

Audit record	Action	Rule
FAU_SAA.1/SYS	inform Admin	Inform Admin if Audit Analyzer starts or stops more than 10 times an hour Inform Admin if Push error occurs and if a Push successful after a Push error
FAU_STG.4/SYS	inform Admin	if the event occurs

[41] PP: [assignment: subset of defined auditable events]

[42] PP: [assignment: any other rule]

FAU_STG.4/CON	inform Admin	if the event occurs
FAU_STG.4/CAL	inform Admin stop meter reading	if the event occurs
FCS_COP.1/TLS	inform Admin (if possible)	more than 10 errors per minute
FCS_CKM.1/TLS	inform Admin (if possible)	if the event occurs
FCS_COP.1/CMS	inform Admin (if possible)	if the event occurs
FCS_CKM.1/CMS	inform Admin (if possible)	if the event occurs
FCS_CKM.1/MTR	inform Admin	if an error occurs
FCS_COP.1/MTR	inform Admin	if an error occurs
FCS_COP.1/HASH	inform Admin	if an error occurs
FDP_ACF.1	inform Admin	if an error occurs
FDP_IFF.1/MTR	inform Admin	if an calibration error occur
FDP_SDI.2	inform Admin	if an error occurs
FIA_AFL.1	inform Admin	if an error occurs
FIA_UAU.2	inform Admin	more than 5 errors per minute
FIA_UAU.6	inform Admin	if an error occurs
FIA_USB.1	inform Admin	if an error occurs
FIA_UID.2	inform Admin	if an error occurs
FPT_FLS.1	inform Admin	if an error occurs
FPT_RPL.1	inform Admin	if an error occurs
FPT_STM.1	inform Admin	if an error occurs
	mark meter data	if time is not reliable
	end of marking meter data	if time synchronisation works again
FPT_TST.1	inform Admin	if an error occurs
FTP_ITC.1/MTR	inform Admin	if an error occurs
FTP_ITC.1/WAN	inform Admin	if an error occurs
FTP_ITC.1/USR	inform Admin	if an error occurs

Table 13: Monitoring Rules

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

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 the system log

FAU_STG.4.1/SYS The TSF shall [overwrite the oldest stored audit records] and [*inform Gateway Administrator*][43] if the **system** audit trail is full.

[43] PP: [assignment: other actions to be taken in case of audit storage failure]

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

Dependencies: FAU_STG.1 Protected audit trail storage

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] level of audit; and

c) [*all audit events as listed in Table 14*[44] *and* [*none*][45]].

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, [*additional information as listed in Table 14 and* [*none*][46]].

Hierarchical to: No other components

Dependencies: FPT_STM.1

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	-
Log is full and will overwrite oldest entries	-

Table 14: 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*] with the capability to read [*all information that are related to them*] from the **consumer** audit records.

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

[44] Table 11 in PP

[45] PP: [assignment: additional events or none]

[46] PP: [assignment: additional events or none]

Dependencies: FAU_GEN.1

Application Note 9 The implementation can be found in chap. 7.4.

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 [*inform Gateway Administrator*][47] 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

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] level of audit; and

c) [*all calibration-relevant information as listed in [BSI-TR-03109-1, Table 43 (section 5.3.1) expanded with [PTB-A 50.8, Table 4-23, (section 4.4) (implementation of Application Note 11)]*][48].

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, [*other audit relevant information as listed in Table 15*][49].

Hierarchical to: No other components

Dependencies: FPT_STM.1

Calibration Relevant Information	Additional Information
self test failed	faulty subsystem
self test success after restart	ID, Hardware-ID, firmware version from smgw
smgw firmware update	firmware version
all changes to meter configuration	ID, all calibration relevant Parameters
loss of power	
Success of time synchronization after restart	correct time
calibration error of a sensor	ID

Table 15: Events for calibration log

[47] PP: [assignment: other actions to be taken in case of audit storage failure]

[48] PP: [assignment: all calibration-relevant information]

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

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*] with the capability to read [*all information*] from the **calibration** audit records.
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] and [*stop the operation*[50] *of the TOE and inform a Gateway Administrator*] if the **calibration** 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 12 The implementation can be found in chap. 7.4.

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 13 The implementation can be found in chap. 7.4.

6.2.5.1.2 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** from unauthorised deletion.
FAU_STG.2.2	The TSF shall be able to [prevent] unauthorised modifications to the stored audit records in ~~**the**~~ **all** audit trail**s**.
FAU_STG.2.3	The TSF shall ensure that [*according to legal regulation given by [BSI-TR-3109] sufficient and adjustable size in defined range of entries in calibration log, system log, consumer log*][51] stored audit records will be maintained when the following conditions occur: [audit storage exhaustion or failure].
Hierarchical to:	FAU_STG.1 Protected audit trail storage
Dependencies:	FAU_GEN.1 Audit data generation

[50] The data acquisition will stop. The access over WAN will work for reading logs.

[51] PP: [assignment: metric for saving audit records]

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*] at all times.

FCO_NRO.2.2 The TSF shall be able to relate the [*key material used for signature*[52]] of the originator of the information, and the [*signature*] 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*]] given [*limitations of the digital signature according to [BSI-TR-03109-1]*].

Hierarchical to: FCO_NRO.1 Selective proof of origin

Dependencies: FIA_UID.1 Timing of identification

Application Note 16: 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.

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

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[

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
with Brainpool and NIST Curves Parameter from [BSI-TR-03116-3, Chapter 4.1]

]**[53]** and specified cryptographic key sizes [*128 bit, 256 bit*]**[54]** that meet the following: [*[RFC 5289], [RFC 5246], [RFC 2104], [FIPS 180-4]*]**[55]**.

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation],
fulfilled by FCS_COP.1/TLSFCS_CKM.4 Cryptographic key destruction

Developer Remark 1: The Interface IF_GW_MTR use
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
The Interface IF_GW_WAN use
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
The Interfaces IF_GW_CON, IF_GW_CLS, IF_GW_SRV use
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Application Note 17: The Security Module is used for parts of the TLS key negotiation.

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*] in accordance with a specified cryptographic algorithm [

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

]**[56]** and cryptographic key sizes [*128 bit, 256 bit*]**[57]** that meet the following: [*[RFC 5289]*, *[RFC 5246]*, *[RFC 2104], [FIPS 197]*, *[FIPS 180-4]*, *[NIST SP800-38A], [NIST SP800-38D]*]**[58]**.

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

53 PP: [assignment: cryptographic key generation algorithm]
54 PP: [assignment: cryptographic key sizes]
55 PP: [assignment: list of standards]
56 PP: [assignment: cryptographic algorithm]
57 PP: [assignment: cryptographic key sizes]
58 PP: [assignment: list of standards]

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

FCS_CKM.4 Cryptographic key destruction

Developer Remark 2: The Interface IF_GW_MTR use
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
The Interface IF_GW_WAN use
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
The Interfaces IF_GW_CON, IF_GW_CLS, IF_GW_SRV use
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

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*][59] and specified cryptographic key sizes [*128 bit, 192 bit, 256 bit*][60] that meet the following: [*[BSI-TR-03111]*][61].

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 22: The TOE utilises the services of its Security Module for parts of the key generation procedure.

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 [

id-aes-CBC-CMAC-128,
id-aes-CBC-CMAC-192,
id-aes-CBC-CMAC-256,
id-aes128-gcm,
id-aes192-gcm,
id-aes256-gcm

][62] and cryptographic key sizes [*128 bit, 192 bit, 256 bit*][63] that meet the following: [*[RFC 5084]*, *[RFC 4493], [RFC 5652], [FIPS 197]*, *[NIST SP800-38A]*, *[NIST SP800-38D]*][64].

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

[59] PP: [assignment: cryptographic key generation algorithm]
[60] PP: [assignment: cryptographic key sizes]
[61] PP: [assignment: list of standards]
[62] PP: [assignment: cryptographic algorithm]
[63] PP: [assignment: cryptographic key sizes]
[64] PP: [assignment: list of standards]

FCS_CKM.1 Cryptographic key generation], fulfilled by FCS_CKM.1/CMS

FCS_CKM.4 Cryptographic key destruction

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*][65] and specified cryptographic key sizes [*128 bit, 2x128bit*][66] that meet the following: [*[RFC 4493], [FIPS 197]*][67].

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

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 and integrity protection*] in accordance with a specified cryptographic algorithm [*AES-CMAC, AES_CBC*][68] and cryptographic key sizes [*128 bit, 2x128bit*][69] that meet the following: [*[RFC 4493]*, *[FIPS 197], [NIST SP800-38A]*][70].

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 29: The PP 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
   a. the key is being generated by the Gateway periodically according to [BSI-TR-03109-3] as defined by FCS_CKM.1/MTR and sent to the Meter via encrypted TLS-channel as defined by FCS_COP.1/TLS or
   b. the key has been brought into the Gateway via a management function during the pairing process for the Meter (see FMT_SMF.1) and defined by FCS_COP.1/MTR.

[65] PP: [assignment: cryptographic key generation algorithm]
[66] PP: [assignment: cryptographic key sizes]
[67] PP: [assignment: list of standards]
[68] PP: [assignment: cryptographic algorithm]
[69] PP: [assignment: cryptographic key sizes]
[70] PP: [assignment: list of standards]

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 [*zeroization*][71] that meets the following: [*[FIPS 140-2]*][72].

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

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*] in accordance with a specified cryptographic algorithm [*SHA-256, SHA-384*][73] and cryptographic key sizes [*none*][74] that meet the following: [*[FIPS 180-4]*][75].

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[76]]

FCS_CKM.4 Cryptographic key destruction

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

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*] in accordance with a specified cryptographic algorithm [*AES-GCM*][77] and cryptographic key sizes [*256 bit*][78] that meet the following: [*[FIPS 197], [NIST SP800-38D]*][79].

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]

FCS_CKM.4 Cryptographic key destruction

---

71 PP: [assignment: cryptographic key destruction method]
72 PP: [assignment: list of standards]
73 PP: [assignment: cryptographic algorithm]
74 PP: [none]
75 PP: [assignment: list of standards]
76 The justification for the missing dependency FCS_CKM.1 can be found in chapter 6.12.1.3
77 PP: [assignment: cryptographic algorithm]
78 PP: [assignment: cryptographic key sizes]
79 PP: [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 [BSI-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*] 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

] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

Hierarchical to: FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 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*] 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

].

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,*
- *[none]*

]**[80]** .

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*]**[81]**.

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*
- **an LMN Meter has no read access to any data**

].

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*] on [*the TOE, external entities on the WAN side, external entities on the LAN side and all in-formation flowing between them*] and all operations that cause that information to flow to and from subjects covered by the SFP.

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*] 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:

80 PP: [assignment: additional rules governing access among controlled subjects and controlled objects using controlled operations on con-trolled objects or none]

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

destination_interface (TOE, LMN, HAN or WAN),
source_interface (TOE, LMN, HAN or WAN),
destination_authenticated,
source_authenticated

].

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

[*if source_interface=TOE and*
(destination_interface=HAN or destination_interface=LMN) and
destination_authenticated = true
Connection establishment is allowed

if (source_interface=LMN or source_interface=HAN) and
destination_interface=TOE and
source_authenticated = true
Connection establishment is allowed][82]

else

Connection establishment is denied

].

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*].

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

FDP_IFF.1.5/FW The TSF shall explicitly deny an information flow based on the following rules: [*none*][83].

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

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*] on *[the TOE, attached Meters, authorized External Entities in the WAN and all information flowing between them*] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2/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

---

82 PP: [assignment: other rules or none]

83 PP: [assignment: rules, based on security attributes that explicitly deny information flows]

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] 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

].

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 Pro*file

].

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 Profile,*
- *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:*
  - *The TOE shall compare the system time to a reliable external time source [according to [RFC 5905] implemented min/max poll intervall between 1 minute and 24 hours]*[84].
  - *If the deviation between the local time and the remote time is acceptable 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*[85] *and*
      - *inform a Gateway Administrator*

].

FDP_IFF.1.4/MTR The TSF shall explicitly authorise an information flow based on the following rules: [*none*][86].

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*].

Hierarchical to: No other components

Dependencies: FDP_IFC.1 Subset information flow control

---

84 PP [assignment: synchronisation interval between 1 minute and 24 hours]

85 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.

86 PP: [assignment: rules, based on security attributes that explicitly authorise information flows]

FMT_MSA.3 Static attribute initialisation

Application Note 44 The implementation can be found in chap. 7.1.

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] all objects.

Hierarchical to: FDP_RIP.1 Subset residual information protection

Dependencies: No dependencies.

Application Note 45: 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 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*][87] on all objects, based on the following attributes: [*cryptographic checksum (HMAC using SHA-256) over the object*][88].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [*perform actions as listed in Table 16*][89].

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

Dependencies: No dependencies.

Data Type	Action
stored meter data	ignore data and create an entry in system log
stored config data	ignore data and create an entry in system log
stored audit data	ignore data and create an entry in system log

Table 16: Actions to be taken in case of detection of integrity errors

See Chapter 6.2.2.3.1 for actions for created log entries.

Application Note 46 The implementation can be found in chap. 7.7.

[87] PP: [assignment: integrity errors]

[88] PP: [assignment: user data attributes]

[89] PP: [assignment: action to be taken]

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*
- *[attributes listed in* Table 17*]*[90]

].

Hierarchical to: No other components.

Dependencies: No dependencies.

User Attribute	Description
activated	The flag is true, if the UserProfile is usable for authentication
blocking flag	The flag is true, if a user is excluded from authentication.
blocking time	The time at which the exclusion occurs
login time	last successfully login time
logout time	last successfully logout time

Table 17: extended User Attribute Definition

6.6.2 Authentication Failure handling (FIA_AFL)

6.6.2.1 FIA_AFL.1: Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when [a ~~**Gateway Administrator configurable**~~ positive integer ~~**of within**~~ [3 ~~**and 10**~~]][91] unsuccessful authentication attempts occur related to [*authentication attempts at IF_GW_CON*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [*block the user for 15 minutes and create a log entry into system log*][92].

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 47 The implementation can be found in chap. 7.2.

[90] PP: [assignment: list of security attributes or none]

[91] security enhancement, only the best security is possible

[92] PP: [assignment: list of actions]

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*
- *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*

] 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*

].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 48 The implementation can be found in chap. 7.2.

6.6.3.3 FIA_UAU.6: Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate **an external entity** 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 10 minutes of inactivity*

].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 49 The implementation can be found in chap. 7.2.

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.

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*].

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: [

- *set user identity to configured value*
- *set status of identity to not authenticated*
- *set connecting network to configured selection (WAN, HAN or LMN)*
- *set role membership to configured selection (Consumer, GWA, Service Technician or Authorised External Entity)*
- *set activation flag to configured selection (true or false)*
- *in case of a new user object set blocking flag to false and blocking time to 0 (1970-01-01 00:00:00)*
- *in case of a configured user object set the blocking flag and blocking time from the stored values*
- *in case of a new user object set login and logout time to 0 (1970-01-01 00:00:00)*
- *in case of a configured user object set the login and logout time to the last stored values.*

]**[93]**.

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: [

- *the user identity cannot change*
- *the status of identity can change (authenticated or not)*
- *the connecting network cannot change*
- *the role membership cannot change*
- *the activation flag can change between true and false to deactivate Consumer or CLS Devices*
- *the blocking flag and blocking time can between true and false change if a Consumer will block because of unsuccessful logins and if the blocking time is expired*
- *the login and logout time can change with the actual timestamp if a Consumer login and logout*

]**[94]**.

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

93 PP: [assignment: rules for the initial association of attributes]

94 PP: [assignment: rules for the changing of attributes]

6.7 Class FMT: Security Management

6.7.1 Management of the TSF

6.7.1.1 Management of functions in TSF

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] the functions [*for management as defined in FMT_SMF.1*] to [*roles and criteria as defined in Table 18*[95]].

Hierarchical to: Not 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.
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[96].
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 18: Restrictions on Management Functions

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 19*[97] *and Table 20*[98] *and [none]*[99]].

Hierarchical to: No other components.

Dependencies: No dependencies.

SFR	Management functionality	Refinement Reason
FAU_ARP.1/SYS	~~**The management (addition, removal, or modification) of actions**~~	fixed specification (inform GWA) in SFR, no choice possible
FAU_GEN.1/SYS FAU_GEN.1/CON FAU_GEN.1/CAL	-	
FAU_SAA.1/SYS	~~**Maintenance of the rules by (adding, modify-**~~	fixed specification of audit events

[95] Table 12 in PP

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

[97] Table 13 in PP

[98] Table 14 in PP

[99] PP: [assignment: additional functionalities]

SFR	Management functionality	Refinement Reason
	~~**ing, deletion) of rules from the set of rules.**~~	in SFR, no choice possible
FAU_SAR.1/SYS FAU_SAR.1/CON FAU_SAR.1/CAL	- [100]	
FAU_STG.4/SYS FAU_STG.4/CON	~~**Maintenance (deletion, modification, addition) of actions to be taken in case of audit storage failure.**~~. Size configuration of the audit trail that is available before the oldest events get overwritten.	fixed specification of the behaviour in the SFR (overwrite the oldest records), no choice possible
FAU_STG.4/CAL	- [101]	
FAU_GEN.2	-	
FAU_STG.2	Maintenance of the parameters that control the audit storage capability for the consumer log and the system log.	
FCO_NRO.2	The management of ~~**changes to information types, fields, originator attributes and recipients**~~ **key material** of evidence.	fixed specification of hash, no choice possible. Only the key material can change.
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**~~	fixed specification of encryption, no possibility to change the key.
FDP_ACC.2	-	
FDP_ACF.1	-	
FDP_IFC.2/FW	-	
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.	fixed specification of attributes in SFR
FDP_IFC.2/MTR	-	

[100] As the rules for audit review are fixed within this ST the management functions as defined by Common Criteria part 2 do not apply.

[101] As the actions that shall be performed if the audit trail is full are fixed within this ST the management functions as defined by Common Criteria part 2 do not apply.

SFR	Management functionality	Refinement Reason
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.**~~	fixed specification of attributes for hash and actions in case of an integrity error in SFR
FIA_ATD.1	If so indicated in the assignment, the authorised Gateway Administrator might be able to define additional security attributes for users.	fixed specification of attributes in SFR
FIA_AFL.1	~~**Management of the threshold for unsuccessful authentication attempts;**~~ ~~**Management of actions to be taken in the event of an authentication failure.**~~	fixed specification of unsuccessful authentication attempts in SFR fixed specification of actions in SFR
FIA_UAU.2	Management of the authentication data by an Gateway Administrator;	
FIA_UAU.5	- [102]	
FIA_UAU.6	- [103]	
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.**~~ ~~**An authorised Gateway Administrator can change subject security attributes, if so indicated in the assignment of FIA_ATD.1.**~~	fixed specification of attributes in SFR
FMT_MOF.1	~~**Managing the group of roles that can interact with the functions in the TSF.**~~	fixed specification of behaviour in SFR
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.**~~	fixed specification of behaviour in SFR
FMT_MSA.3/AC	- [104]	
FMT_MSA.1/FW	~~**Management of rules by which security attributes inherit specified values.**~~	fixed specification of behaviour in SFR
FMT_MSA.3/FW	- [105]	
FMT_MSA.1/MTR	~~**Management of rules by which security attributes inherit specified values.**~~	fixed specification of behaviour in SFR
FMT_MSA.3/MTR	- [106]	

[102] As the rules for re-authentication are fixed within this ST the management functions as defined by Common Criteria part 2 do not apply.

[103] As the rules for re-authentication are fixed within this ST the management functions as defined by Common Criteria part 2 do not apply.

[104] As no role is allowed to specify alternative initial values within this ST the management functions as defined by Common Criteria part 2 do not apply.

[105] As no role is allowed to specify alternative initial values within this ST the management functions as defined by Common Criteria part 2 do not apply.

[106] As no role is allowed to specify alternative initial values within this ST the management functions as defined

SFR	Management functionality	Refinement Reason
FPR_CON.1	~~**Definition of the interval in FAU_CON.1.2 if definable within the operational phase of the TOE**~~	The definition of the interval is definable by the GWA with the Meter configuration. The transfer interval to the EMT is definable by the GWA A direct definition of packet size an transfer time is not possible.
FPR_PSE.1	-	
FPT_FLS.1	-	
FPT_RPL.1	-	
FPT_STM.1	~~**Management of a time source.**~~	The timesource is always the GWA through the channel admin-service.
FPT_TST.1	- [107]	
FPT_PHP.1	~~**Management of the user or role that determines whether physical tampering has occurred.**~~	The passive detection by the device is not possible, because a security label is used.
FTP_ITC.1/WAN	- [108]	
FTP_ITC.1/MTR	- [107]	
FTP_ITC.1/USR	- [107]	

Table 19: SFR related Management Functionalities

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[109]

Table 20: 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 external entity from section 3.1 (External entities)]][110]

by Common Criteria part 2 do not apply.

[107] As the rules for TSF testing are fixed within this ST the management functions as defined by Common Criteria part 2 do not apply.

[108] As the configuration of the actions that require a trusted channel is fixed by the ST the management functions as defined in part 2 of Common Criteria do not apply.

[109] 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**~~. Reason: at full filled calibration log reading the meter interface will stopped. This state is irreversible and persistent.

].

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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*] to restrict the ability to [query, modify, delete, [*none*][111]] the security attributes [*all relevant security attributes*] to [*authorised Gateway Administrators*].

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*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/AC The TSF shall allow the [*no role*] 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

6.7.4 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*] to restrict the ability to [query, modify, delete, [*none*][112]] the security attributes [*all relevant security attributes*] to [*authorised Gateway Administrators*].

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*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

---

[110] PP: [assignment: the authorised identified roles]

[111] PP: [assignment: other operations]

[112] PP: [assignment: other operations]

FMT_MSA.3.2/FW	The TSF shall allow the [*no role*] 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 52 The implementation can be found in chap. 7.5.

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*] to restrict the ability to [change_default, query, modify, delete, [*none*][113]] the security attributes [*all relevant security attributes*] to [*authorised Gateway Administrators*].
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

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

FMT_MSA.3.1/MTR	The TSF shall enforce the [*Meter SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/MTR	The TSF shall allow the [*no role*] 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

[113] PP: [assignment: other operations]

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*] in order to ensure that no personally identifiable information (PII) can be obtained by an analysis of [*packet size, transfer time, randomly sent packets with dynamic size*][114].

FPR_CON.1.2 The TSF shall connect to [*external entity Gateway Administrator, Authorized External Entity (see 3.1 External entities) speaking literally LMN-Meters, CLS-Devices, EMT, GWA*][115] in intervals as follows [[*intervals configured by GWA from 60 seconds up to 2 days in 900 seconds steps*]][116] to conceal the data flow.

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*] 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*].

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

FPR_PSE.1.3 The TSF shall [determine an alias for a user] and verify that it conforms to the [*replacement of user attribute in measurement data*][117].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 54 The implementation can be found in chap. 7.3.

[114] PP: [assignment: characteristics of the information flow that need to be concealed]

[115] PP: [assignment: list of external entities]

[116] PP: [selection: weekly, daily, hourly, [assignment: other interval]]

[117] PP: [assignment: alias metric]

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,*
- *[unavailable system resources,*
  file system errors,
  uncontrolled failures of subsystems(like crashes)][118]

].

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 55 The implementation can be found in chap. 7.6.

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*].

FPT_RPL.1.2 The TSF shall perform [*ignore replayed data*] 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.

Application Note 56 The implementation can be found in chap. 7.6.

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] to demonstrate the correct operation of [the TSF].

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

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

Hierarchical to: No other components.

Dependencies: No dependencies.

Application Note 57 The implementation can be found in chap.7.6.

[118] PP: [assignment: other of types of failures in the TSF]

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's 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.
FTP_ITC.1.2/WAN	The TSF shall permit [the TSF] 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*].
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, the TOE**][119] 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*].
Hierarchical to:	No other components.
Dependencies:	No dependencies

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 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**] 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*].
Hierarchical to:	No other components.
Dependencies:	No dependencies.

[119] PP: [selection: the Meter, the TOE]

6.11 Security Assurance Requirements for the TOE

The minimum Evaluation Assurance Level for this Protection Profile 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
	ALC_CMS.4
	ALC_DEL.1
	ALC_DVS.1
	ALC_LCD.1
	ALC_TAT.1
	ALC_FLR.2
Security Target Evaluation	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
Tests	ATE_COV.2
	ATE_DPT.1
	ATE_FUN.1
	ATE_IND.2
Vulnerability Assessment	AVA_VAN.5

Table 21: 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.Management	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						
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								

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Management	O.Log	O.Access
FDP_IFC.2/MTR				X		X				
FDP_IFF.1/MTR				X		X				
FDP_RIP.2							X			
FDP_SDI.2							X			
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		
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			
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 22: 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 LMN 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**
  ensures 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 pseudonymisation 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 authorises 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 Administrator 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 PP 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.1
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

SFR	Dependencies	Fulfilled by
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 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/MTR FCS_CKM.4
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	FCS_CKM.4 Please refer to chapter 6.12.1.3 for missing dependency
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	FCS_CKM.4 Please refer to chapter 6.12.1.3 for missing dependency
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
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

SFR	Dependencies	Fulfilled by
FMT_MOF.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR1 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 FMT_SMF.1 Specification of Management Functions	FDP_ACC.2 FMT_SMR.1 FMT_SMF.1
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/FW 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 23: SFR Dependencies

6.12.1.3 Justification for missing dependencies

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.

The key material as defined in FCS_COP.1/MEM will be generated and stored into the security module while the integration phase of production of the TOE. There is no dependency to SFR FCS_CKM.1/CMS.

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 Protection Profile 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

This chapter presents the security functions implemented by the TOE.

7.1 SF.CR: Cryptographic Support

The TOE implements the cryptographic functionality as required by Annex A of [BSI-TR-3109]. As defined by [SMGW-PP] this functionality covers the symmetric parts of the required cryptographic primitives.

The TOE specifically implements the following algorithms for different purposes (other algorithms as defined by FCS_COP.1/* aren't supported):

Purpose	SFR	Algorithm	Key sizes
TLS communication WAN / HAN / LMN wired (incl. key generation)	FCS_CKM.1/TLS FCS_COP.1/TLS	AES-CBC/AES-GCM AES-CBC/AES-GCM	128,256 Bit 128,256 Bit
LMN wireless communication (incl. key generation)	FCS_CKM.1/MTR FCS_COP.1/MTR	AES-CMAC AES-CBC/AES-CMAC	128,2x128 Bit 128,2x128 Bit
Communication content encryption (CMS, incl. key generation)	FCS_CKM.1/CMS FCS_COP.1/CMS	ECKA-EG AES-CBC/AES-CMAC AES-CBC/AES-GCM	128,192,256,512 Bit 256 bit
TSF and user data encryption	FCS_COP.1/MEM	AES-GCM	128 Bit
Hashing for digital signatures	FCS_COP.1/HASH	SHA-256, SHA-384	-
Key destruction	FCS_CKM.4	Zeroization	-

Table 24: Cryptographic primitives

The TOE utilizes the services of the security module ([SM-PP]) for all asymmetric cryptographic primitives.

The TOE encrypts all TSF and user data if they are not in use.

The TOE will use the Security Module to generate all necessary random numbers.

In case of an error or an abnormality a log entry will be created and a Gateway Administrator will be informed according to the monitoring rules of FAU_SAA.1/SYS (chap. 6.2.2.3).

The additional encryption for IF_GW_WAN is done with the private WAN.ENC key and the signature is created with the WAN.SIG certificate (FCS_CKM.1/CMS).

Abnormalities are logged to the system log and in some cases an event is sent to the Gateway Administrator (FAU_SAA.1/SYS) following the rules in chap. 6.2.2.3.

Hashes and Signatures

Hashes are used for the integrity protection of measurement data (recorded, derived and stored), log data and CMS containers (FCS_COP.1/HASH). Signatures are added to measurement data to proof their origin (FCO_NRO.2).

File System Encryption

According to [BSI-TR-03116-3] file contents and file attributes stored in the persistent memory are encrypted (FCS_COP.1/MEM). The used parameters are:

cipher AES-265-GCM
compression LZO

7.1.1 Used TLS Parameters

Used parameters for the TLS connections on the interfaces IF_GW_WAN, IF_GW_CON, IF_GW_SRV, IF_GW_CLS, IF_GW_MTR (FCS_CKM.1/TLS):

Version: 1.2
key exchange ECDHE-ECDSA

Cipher	AES-128-CBC AES-256-CBC AES-128-GCM AES-256-GCM
MAC	SHA256 SHA384
compression	none
Certificate with ECC keys curves	SECP256R1 (NIST P-256) SECP384R1 (NIST P-384) BrainpoolP256r1 BrainpoolP384r1 BrainpoolP512r1 [BSI-TR-03109-3 with client and server authentication

Meters are connected via the interface IF_GW_MTR with two different methods (FDP_IFF.1.5/MTR, Application Note 44). Other methods are not supported.

Wired connection on the LMN485 bus, which establishes a TLS connection between meter and SMGw (FCS_COP.1/TLS).

Wireless connection via wM-Bus, which is protected with a symmetrical key (FCS_COP.1/MTR).

7.2 SF.IA: Identification and Authentication

The TOE has to identify/authenticate every user and external entity before allowing any other action on behalf of that user (FIA_ATD.1, FIA_UAU.2, FIA_UID.2). User identities have the following security attributes (FIA_USB.1): identity, status of identity, connecting network, role membership, blocking flag, login and logout time. The Gateway Administrator can configure Consumers with a username/password combination based identification/authentication or with a certificate based identification/authentication. The Gateway Administrator can configure Service Technicians only with a certificate based identification/authentication.

The TOE implements an authentication failure handling mechanism (FIA_AFL.1), when the defined number of unsuccessful authentication attempts has been met, the TSF blocks the user for 15 minutes. There is a separate Timer for each blocked user.

All connections to external entities are formed as TLS channel (FIA_UAU.5), which will re-authenticate under special conditions (FIA_UAU.6) time, transfer volume and inactivity. The TLS channel will re-authenticate by a complete re-connection of the connection. All underlying connections (TCP or HDLC) will re-connect, too.

Connection Reset

The connections are only allowed to be established under the following conditions (FIA_UAU.6):

IF_GW_WAN	max. 48h
IF_GW_CON	min. 10 minutes of inactivity
IF_GW_SRV	min. 10 minutes of inactivity
IF_GW_CLS	min. 10 minutes of inactivity
IF_GW_MTR	max. 5MB of transferred data

The user and roles are configurable as described in FMT_SMR.1.

The following Table shows the context from external Interfaces to the possibility of authentication of users/roles and the count of simultaneously connections.

Network	Interface	Connection (Source -> Destination)	Count
WAN	IF_GW_WAN	SMGW -> Gateway Administrator (Admin) SMGW -> Gateway Administrator (Service) Gateway Administrator (wakeup) -> SMGW SMGW -> External Entity (EMT)	0…1 0…1 0…1 0…32
HAN	IF_GW_SRV	Service Technician ->SMGW	0…1
	IF_GW_CLS	SMGW -> Local Systems	0…16
	IF_GW_CON	Local Consumer -> SMGW	0…32
LMN	IF_GW_MTR	SMGW -> LMN (wired) LMN (wireless) -> SMGW	0…32 0…32[120]

Table 25: external interfaces and simultaneously connections

Other connections or using other interfaces for a specific connection than listed in Table 25 are not allowed.

In case of authentication failure (FIA_AFL.1) or an abnormality a log entry will be created and a Gateway Administrator will be informed according to the monitoring rules of FAU_SAA.1/SYS (chap. 6.2.2.3).

Before executing an action on the SMGw, the user has to be identified/authenticated. Therefore the SMGw checks the transmitted certificates

[120] The count of wireless Meters is limited due to capacity of simultaneously wireless connections in the air. Think about collisions and other low level topics.

of the TLS connection according to [BSI-TR-03109-1]. If an error occurs, no further actions will be executed in the gateway, the TLS connection and the underlying layers will be disconnected. Meters are handled as users too, their connections are also identified/authenticated by certificates. For wireless communicating meters the identification/authentication is performed by a symmetrical key (FCS_COP.1/MTR).

An exception is the consumer, who is also able to identify/authenticate himself with a combination of username and password (FIA_UAU.5). An encrypted TLS connection is still used, but in this case the certificates are not used for the identification/authentication.
Another exception are wireless meters. They are communicating unidirectional with the SMGw (from the meter to the SMGw). They identify/authenticate themselves with their symmetric key.

The identification/authentication of a wakeup requester (Gateway Administrator) is performed by validating the attached signature (FIA_UAU.5).

Identification

The identification of the user (FIA_UID.2) is performed with the following mechanisms:

IF_GW_WAN — A connection is established by the SMGw.
The connection to the Gateway Administrator is established via admin-management.

Via admin-service and EMT no requests towards the SMGw are allowed so the user identification can be omitted.

IF_GW_CON — The identification is done with the provided certificate or the (configured) combination of username and password.

IF_GW_SRV — The identification is done with the provided certificate.

7.3 SF.PR: Privacy

The TOE provides mechanisms for communication concealing (FPR_CON.1) and pseudonymity (FPR_PSE.1).

The pseudonymization is used for TAF 10. The pseudonym to use is provided by the GWA. If a pseudonym is provided, the meter-ID or ID of an evaluation profile that can be assigned to a consumer will be replaced by this pseudonym.
TAF10 is not implemented in the current version of the SMGw.

The SMGw itself will not create a pseudonym.

The Communication to external Entities (see 3.1) is performed over packet oriented networks. To conceal the communication the packet size will be mutable (FPR_CON.1.1), also the transmitted content is padded to random size. This mechanism is used to conceal the transmission size and transmission duration on the interfaces IF_GW_WAN, IF_GW_CON, IF_GW_SRV, IF_GW_CLS and IF_GW_MTR. To conceal the transfer time the SMGW establishes random connections between the normal data transfer with dynamic size of irrelevant data to an external entity in the WAN.

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 link to the identity of the consumer.

In this case the submitted data contains no link to the consumer ID, but a special pseudonymous identifier e.g. GRID. This replacement is only used in the implementation of TAF10 [BSI-TR-03109-1, 4.2.4.1],

For the transmission of billing relevant data the Consumer ID is necessary. In this case a link to a Consumer Profile will contains to the transmitted metering data. There is no name of the real consumer in this link. The Consumer ID is arbitrary to the Gateway Administrator respectively the Gateway Administrator can determine their nomenclature, e.g. numbers only or a mixture from numbers with letters in any form.

7.4 SF.AU: Security Audit

The TOE implements three different audit logs:

Audit messages are assigned to the causing user.

An audit entry contains the following information: domain (log name), date, time, event type, level, subject identity, operation result, causing component, description.

- **System Log** to log all system relevant events on specific functionality and all events as defined by Common Criteria for the used SFRs (FAU_GEN.1/SYS, s. chap. 6.2.2.3, FAU_GEN.2). These events are actions on the interfaces IF_GW_WAN, IF_GW_CON, IF_GW_SRV, IF_GW_CLS and IF_GW_MTR. Consumer related data isn't stored in the system log. The TOE uses a cyclic analysis of the system log to inform the Gateway Administrator (FAU_ARP.1/SYS) about security relevant events according to the monitoring rules (FAU_SAA.1/SYS, s. chap. 6.2.2.3.1). The system log can be read only by the Gateway Administrator and Service Technicians (FAU_SAR.1/SYS). The log is realized as a ring buffer, i.e., after a configurable maximum number of events are added to the log, the TOE begins overwriting the oldest log entries (FAU_STG.4/SYS). The Gateway Administrator is informed every time when the maximum amount of events has been written to the log.
- **Consumer Log** to enable informing the consumer about information flows to the WAN, active access control profiles, all billing-relevant data needed to verify an invoice and not billing-relevant metering data (FAU_GEN.1/CON, see also [BSI-TR-03109-1, Table 44, chapter 5.3.2, page 128/129], FAU_GEN.2). The TOE protects the integrity of the consumer log with a signature. The consumer log can be read only by the Consumer (FAU_SAR.1/CON). A consumer is allowed to read only the entries assigned to him.

  The consumer log contains all entries that are required for a billing verification. This includes the configuration of meters and evaluation profiles, tariff switch points and sent data.

  The log is realized as a ring buffer, i.e., after a configurable maximum number of events are added to the log, the TOE begins overwriting the oldest log entries (FAU_STG.4/CON).The Gateway Administrator is informed every time when the maximum amount of events has been written to the log.
  If a consumer is deleted, his log events are no longer accessible. A deletion of a consumer is only possible if a legally defined time of his associated evaluation profile is elapsed.
- **Calibration Log** to log changes that are relevant for the calibration of the TOE (FAU_GEN.1/CAL, see also [BSI-TR-03109-1, Table 43, chapter 5.3.1, page 128], FAU_GEN.2). The calibration log can only be read by the Gateway Administrator (FAU_SAR.1/CAL). The TOE stops operation (data collection) if the calibration log is full (FAU_STG.4/CAL).

  The size of the calibration log is sufficient for storing messages of the life cycle of the device. A separate memory is used to prevent dependencies to configured meters and evaluation profiles and their memory demand.

If an action is executed in a user context the log event will be associated with this user (FAU_GEN.2). For consumer or service technician the user name is attached to the log entry. The internal users (GWA, EMT, meter) are used if an action is executed in their context.

The logging functionality is implemented as a TOE subsystem. The maximum size of log entries and the resulting actions in case of an error will described by FAU_STG.2.

Log events shall not be modified after storing them.

7.5 SF.SM: Security Management

The TOE provides security management functions only to authorized users (FMT_MOF.1, FMT_SMF.1 and FMT_MSA.1/AC).

Consumer The consumer (authorization via IF_GW_CON) can only display the current version number of the TOE and the current time (FMT_MOF.1).

Service Technician The Service Technician (authorization via IF_GW_SRV) can only change the parameters for the network access for WAN (LTE or IP Parameters) during the installation process. After this, the Service Technician cannot change any Parameters.

Gateway Administrator The Management functions for the Gateway Administrator contains the configuration of all aspects of the SMGW and are only accessible at IF_GW_WAN via a documented protocol.

- Roles und Users (FMT_SMR.1)
- Security Attributes for the Gateway Access Policy (FMT_MSA.1/AC)
- Security Attributes for the Firewall Policy (FMT_MSA.1/FW)
- Security Attributes for the Meter Policy (FMT_MSA.1/MTR)

There are some other tasks, which are carried out by the Gateway Administrator.

- Pairing of a Meter
- Firmware update of Meter
- Firmware update of SMGW
- Management of certificates of external Parties for communication in WAN or HAN
- Resetting TOE
- Start self test

Not allowed for the Gateway Administrator are:

- access to measurement data of a consumer
- access to the consumer log
- deletions within logs

All rules and objects have defined initial states during the startup of the SMGW (FMT_MSA.3/AC, FMT_MSA.3/FW, FMT_MSA.3/MTR). All initial states are hard-coded in the source codes. There is no way to change them.

The initial states respect the rules of FDP_IFF.1.2/FW and FDP_IFF.1.5/FW and accept only the described connections. These rules apply to all information flows and cannot be changed.

Firewall The firewall cannot be configured directly. The configuration is done with the configuration of profiles that influences the firewall (FMT_MSA.1/FW):

- WAN profiles: opening ports for outgoing connections via IF_GW_WAN to the Gateway Administrator and EMT
- HAN profiles: opening ports for incoming connections via IF_GW_CON and IF_GW_SRV for a consumer or the service technician
- HAN profiles: opening ports for incoming or outgoing connections via IF_GW_CLS for CLS devices
- Wakeup profiles: opening port for incoming connections via IF_GW_WAN for the Gateway Administrator to send wakeup requests

At startup of the SMGw the firewall is configured to reject every access to the SMGw. After loading the configured profiles the required ports will be opened (FMT_MSA.3/FW). If a profile is deleted, the associated firewall rule will be deleted too.

Meter Data Incoming Meter data will be received, checked and stored (FDP_IFF.1/MTR). While the calculation of generated meter data via processing profiles the SMGw assigns an unambiguous and reliable timestamp to this data (FPT_STM.1). Using the external time source, the GWA provides by the admin-service channel, a sufficient exactness of the system time of the TOE will be offered. The TOE is using NTP (s. [RFC5905]) to synchronize the system time of the operating system of the TOE periodically. Even if the synchronization process failed (following after a successful time synchronization), the internal clock of the TOE offers a sufficient exactness for another 48h to stay below the maximum time deviation of 3% of the minimum measuring period. The evidence of origin is given by a signature (FCO_NRO.2) which will be calculated by the security module.

7.6 SF.SP: Self-Protection

The TOE implements functionality for self-protection. The TOE preserves a secure state in case of failures (FPT_FLS.1). If there is no reliable time stamp available all recorded measurement data will marked, that the EMT will learn this. The TOE detects replay of specific data (FPT_RPL.1) on the TLS layer with protocol inspection [RFC5246, F.2 Protecting Application Data]. The TOE provides reliable time stamps based on NTP (FPT_STM.1) which are provided by the GWA via the admin-service channel. The TOE runs a suite of self tests during initial startup, at the request of a user and periodically during normal operation (FPT_TST.1). The TOE housing is sealed in order to allow a detection of a physical attack (FPT_PHP.1). The seal meets the requirements from [BSI-TL-0345], securitly level 2:

- no seal removal without destroying the seal
- protection against thermal removal
- protection against chemical removal (ethyl alcohol, solvent)

The SMGW implements a monitor for processes, to detect malfunctions. In this case a subsystem will be re-started (FPT_FLS.1.1) and the internal connections will be re-established. If a malfunction occurs several times in a short time or if the process monitoring itself is faulted, the whole SMGw will be restarted.

The clock may differ max. 3% from the smallest registering period (15 minutes) according to [PTB-A 50.8]. The TOE monitors the state of time synchronization periodically. If the TOE lost the state of time synchronization or time synchronization fails after start-up, newly recorded and stored metering data will be tagged, so they cannot be used for billing anymore.

For the synchronization with the legal time only the admin service channel to the Gateway Administrator is used. The Gateway Administrator has to make sure that the time is obtained from a trustworthy source.

The Audit function described above informs the Gateway Administrator in case of an error (see 7.4, SF.AU: Security Audit, FAU_ARP1/SYS).

self test The SMGW implements several self tests which will execute at system startup and on request by GWA/Service Technician/Consumer and periodically during normal operation. Each subsystem has its own test, so only the success of all test results into a proper SMGw, which collects and send flawless measurement data. The tests contain (depending on scenario/user):

- status of resources (persistent and volatile)
- status of physical interfaces
- status of logical interfaces
- integrity of stored data
- integrity of firmware
- status of security module
- deviation of the clock time
- check if the interfaces for WAN an LAN are separate
- detection of repetitions in the TLS layer (FPT_RPL.1)

The test for separation of the interfaces WAN and HAN is done by trying to reach the GWA via the HAN interface. If this is possible a misconfiguration is detected.

7.7 SF.UD: User Data Protection

The TOE provides functionality to logically remove unused information (FDP_RIP.2) by zeroization. An access to deleted data is not possible.

Generally all unused objects in the memory (volatile and non-volatile) are released. The software architecture prevents direct access to the memory. The only possibility to access objects is via HTTP methods. The HTTP requests are validated in the software, which ensures that only existing objects can be accessed. Access to not/no longer existing objects causes errors.

The integrity protection of configuration- and meter data objects is done with a hash. The checksum is created on the creation of the related object and stored with it. On every read process of this object from the non-volatile memory the signature is checked. The object is only processed if this check was successful. In case of a failed check an entry is created in the system log and the gateway administrator is informed.
The anchor of trust comes from the file system encryption that also secures the configuration- and meter data objects. The key for the file system encryption is provided by the integrated security module.
The TOE detects integrity errors of persistently stored configuration and meter data and informs the Gateway Administrator accordingly (FDP_SDI.2).

The TOE communicates with meters (FTP_ITC.1/MTR), WAN participants (FTP_ITC.1/WAN), users (FTP_ITC.1/USR) via trusted paths/trusted channels only. Channels on different physical interfaces are physically separated from each other and channels on the same physical interfaces are logically separated from each other.

Access control policy The TOE implements one access control policy:

Gateway Access SFP The TOE implements the **Gateway Access SFP** (see 6.5.2). This SFP is an access control policy controlling the access by the Gateway Administrator and Consumer on meter data, on the configuration and on the different audit logs (FDP_ACC.2, FDP_ACF.1).

Transmitted profiles are checked for correctness during the parameterization process of the SMGw. [FDP_ACC.2] implements access permissions.
The transmitted (evaluation) profiles define which data is transferred to an external entity at which time. They also contain information about the amount of processing of data. A user, whose id is also part of the profile, can access only the profiles related to him.
Please refer to chap. 7.3 to check if the data is pseudonymised.

The access control functionality is implemented as mandatory access control via SELinux. SELinux confines users and processes to the minimum amount of privilege they require. This reduces the ability of these users and processes to cause harm when compromised. The SELinux access control mechanism operates on top of the traditional Linux access control mechanism. The basis for the SELinux access control mechanism is a policy loaded on the system, which gives each user and process of the system only the access to objects they require to function. There’s no possibility to read or change the policies. The TOE implements a targeted policy which confines selected system processes only. All other processes run in an unconfined domain and are not covered by the SELinux protection model.

Flow control policies The TOE implements two different information flow control policies:

Firewall SFP This policy controls the communication among the TOE and the different networks. Consequently, the TOE implements physically separate interfaces for WAN, LMN and HAN communication. As illustrated in Figure 7, the TOE realizes the following rules (FDP_IFC.2/FW, FDP_IFF.1/FW):

Gateway The gateway itself

- connection establishment to the WAN is allowed – using only pre-configured addresses
- connection establishment to the HAN is allowed
- connection establishment to the LMN is allowed
- the Gateway offer a wake-up service (trigger a connection establishment by the Gateway)
- only cryptographically-protected connections are possible

Firewall The firewall is a component in the gateway. The functionality is provided via Linux's iptables firewall policies.

- only connections established from internal network to external network are allowed
- a wake-up service on the WAN side interface is provided
- communication from CLS in the HAN to the WAN are allowed only if confidentiality-protected and integrity-protected and if endpoints are authenticated

WAN The external party (Gateway Administrator, EMT) on the WAN side (see 3.1.)

- connection establishment to the LMN is not allowed
- connection establishment to the Gateway is not allowed
- connection establishment is allowed to trustworthy, pre-configured endpoints and via an encrypted channel only

HAN The external party (Consumer, Service Technician, CLS device) on the local side (see 3.1)

- connection establishment to the WAN is not allowed
- connection establishment to the LMN is not allowed
- devices in the HAN may communicate with each other (however, the Gateway is not involved)
- communications between devices within different HAN via the TOE are only allowed if explicitly configured by a Gateway Administrator
-

LMN The external party (meter) on the LMN side

- connection establishment to the WAN is not allowed
- connection establishment to the HAN is not allowed
- no communications between devices in the LMN are assumed, they shall not be connected to any other network

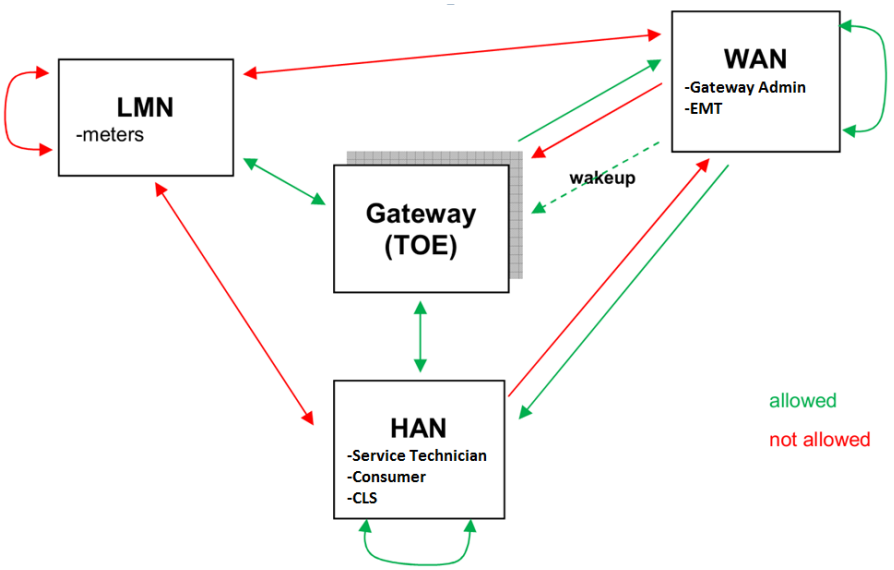

Figure 7: Firewall SFP Concept

Data access The access to data depends on the user role (FDP_ACF.1). Users can connect only with an interface that is desired for his user role (FMT_SMR.1).

Gateway Administrator Connects via IF_GW_WAN.

- access to configuration profiles is allowed
- access to consumer data (measurement data, consumer log entries) is not allowed
- initiating a reboot or self test is allowed

EMT Connects via IF_GW_WAN

- receiving of measurement data, if configured, is allowed
- access to any other data is not allowed

Consumer Connects via IF_GW_CON

- access to profiles assigned to him is allowed
- access to log entries assigned to him is allowed
- access to all other data is not allowed
- initiating a self test is allowed

Service Technician Connects via IF_GW_SRV

- access to WAN network parameters during the installation process is allowed
- access to WAN network parameters after the installation process is not allowed
- access to log, status- and version-information is allowed
- initiating a reboot or self test is allowed
- access to consumer data (measurement data, consumer log entries) is not allowed

CLS device Connects via IF_GW_CLS

- access to data is not allowed

Meter Connects via IF_GW_MTR

- access to data is not allowed

Meter SFP Governs the handling of Meter Data (FDP_IFC.2/MTR). The behaviour of this functionality is based on access control profiles as part of the configuration of the Gateway (FDP_IFF.1/MTR). Without a profile for a meter, the meter is simply visible for the SMGw but no meter data will be collected from it. A direct connection to other interfaces than IF_GW_LMN isn't allowed.

7.8 Rationale on TOE Specifications

	SF.CR	SF.IA	SF.PR	SF.AU	SF.SM	SF.SP	SF.UD
FAU_ARP.1/SYS				X			
FAU_GEN.1/SYS				X			
FAU_SAA.1/SYS	X	X		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				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						
FCS_COP.1/MTR	X						
FCS_CKM.4	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						X
FDP_IFC.2/MTR							X
FDP_IFF.1/MTR					X		X
FDP_RIP.2							X
FDP_SDI.2							X
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					
FMT_MOF.1					X		
FMT_SMF.1					X		
FMT_SMR.1		X			X		X
FMT_MSA.1/AC					X		
FMT_MSA.3/AC					X		

	SF.CR	SF.IA	SF.PR	SF.AU	SF.SM	SF.SP	SF.UD
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	
FPT_RPL.1						X	
FPT_STM.1					X	X	
FPT_TST.1						X	
FPT_PHP.1						X	
FTP_ITC.1/WAN							X
FTP_ITC.1/MTR							X
FTP_ITC.1/USR							X

Table 26: Coverage of SFRs

8 Appendix

8.1 Mapping from English to German terms

	The Mapping contains the English term on the left and the german meaning on the right side
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 Netz (für Kommunikation)
LMN, Local Metrological Network	Lokales Messeinrichtungsnetz
Meter	Messeinrichtung (Teil eines Messsystems)
Processing Profiles	Konfigurationsprofile
Security Module	Sicherheitsmodul (z.B. eine Smart Card)
Service Provider	Dienstanbieter
Smart Meter / Smart Metering System	Intelligente, in ein Kommunikationsnetz eingebundene, elektronische Messeinrichtung (Messsytem)
TOE	EVG (Evaluierungsgegenstand)
WAN, Wide Area Network	Weitverkehrsnetz (für Kommunikation)

8.2 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])
CA	Certificate Authority or Certification Authority, an entity that issues digital certificates.
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
DTBS	Data To Be Signed
EAL	Evaluation Assurance Level
Energy Service Provider	Organisation offering energy related services to the consumer (according to [CEN])
external entity	See chapter 3.1
firmware update	See chapter 3.2
Gateway Administrator	See chapter 3.1
Gateway config (secondary asset)	See chapter 3.2
Gateway time	See chapter 3.2
Home Area Network (HAN)	In-house LAN which interconnects domestic equipment and can be used for energy management purposes. (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
LAN	Local Area Network
Local attacker	See chapter 3.4
Meter config (secondary asset)	See chapter 3.2
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).

Term	Description
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.
Service Technician	See chapter 3.1
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])
TLS	Transport Layer Security protocol according to RFC5246
TOE	Target of Evaluation - set of software, firmware and/or hardware possibly accompanied by guidance
TSF	TOE security functionality
WAN attacker	See chapter 3.4
WLAN	Wireless Local Area Network

8.3 References

[AIS20] Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, BSI, current version

[AIS31] Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, BSI, current version

[BSI-TL-03415] BSI TL-03415, BSI, Stand Sep. 2015
Anforderungen und Prüfbedingungen für Sicherheitsetikette (BSI 7586)
Ver.: 1.0

[BSI-TR-02102] BSI TR-02102-2, BSI, current version,
Kryptographische Verfahren: Empfehlungen und Schlüssellängen

[BSI-TR-03109] BSI TR-03109, BSI, current version

[BSI-TR-03109-1] BSI TR-03109-1, BSI, current version,
Anforderungen an die Interoperabilität der Kommunikationseinheit eines Messsystems

[BSI-TR-03109-2] BSI TR-03109-2, BSI, current version,
Smart Meter Gateway – Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls

[BSI-TR-03109-3] BSI TR-03109-3, BSI, current version,
Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen

[BSI TR-03116-3] BSI TR-03116-4, BSI, current version,
eCard-Projekte der Bundesregierung – Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen

[BSI-TR-03109-4] BSI TR-03109-4, BSI, current version,
Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways

[BSI-TR-03109-1-I] BSI TR-03109-1 Anlage I, BSI, current version,
CMS Datenformat für die Inhaltsdatenverschlüsselung und -signatur

[BSI-TR-03109-1-II] BSI TR-03109-1 Anlage II, BSI, current version,
COSEM/http Webservices

[BSI-TR-03109-1-IIIa] BSI TR-03109-1 Anlage IIIa, BSI, current version,
Feinspezifikation „Drahtlose LMN-Schnittstelle“ Teil 1

[BSI-TR-03109-1-IIIb] BSI TR-03109-1 Anlage IIIb, BSI, current version,
Feinspezifikation „Drahtlose LMN-Schnittstelle“ Teil 2

[BSI-TR-03109-1-IV] BSI TR-03109-1 Anlage IV, BSI, current version,
Feinspezifikation „Drahtgebundene LMN-Schnittstelle“

[BSI-TR-03109-1-V] BSI TR-03109-1 Anlage V, BSI, current version,
Anforderungen zum Betrieb beim Administrator

[BSI-TR-03109-1-VI] BSI TR-03109-1 Anlage VI, BSI, current version,
Betriebsprozesse

[BSI-TR-03111] BSI TR-03111, BSI, current version,
Elliptic Curve Cryptography

[CC] Common Criteria for Information Technology Security Evaluation –

- Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 4
- Part 2: Security functional requirements, dated September 2012, version 3.1, Revision 4
- Part 3: Security assurance requirements, dated September 2012, version 3.1, Revision 4

[CEN]	SMART METERS COORDINATION GROUP (SM-CG) Item 5. M/441 first phase deliverable – Communication – Annex: Glossary (SMCG/Sec0022/DC)
[FIPS 180-4]	Federal Information Processing Standards Publication 180-4 Secure Hash Standard (SHS), 2015
[FIPS 197]	Federal Information Processing Standards Publication 197 Advanced Encryption Standard (AES), 2001
[NIST SP800-38A]	NIST Special Publication 800-38A, Morris Dworkin, Recommentation for Block Cipher Modes of Operation, Methods andTechniques, 2001
[NIST SP800-38D]	NIST Special Publication 800-38D, Morris Dworkin, Recommentation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, 2007
[RFC 2104]	IETF RFC 2104, H. Krawczyk, M. Bellare, R. Canetti, HMAC: Keyed-Hashing for Message Authentication, 1997
[RFC 4493]	IETF RFC 4493, JH. Song, R. Poovendran, The AES-CMAC Algorithm, 2006
[RFC 5246]	IETF RFC 5246, T. Dierks: The Transport Layer Security (TLS) Protocol Version 1.2, 2008
[RFC 5289]	IETF RFC 5289, M. Rescorla: TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (CGM), 2008
[RFC 5084]	IETF RFC 5084. R. Housley: Using AES-CCM and AES-CGM Authenticated Encryption in the Cryptographic Message Syntax (CMS)
[RFC 5905]	IETF RFC 5905, D. Mills: Network Time Protocol Version 4: Protocol and Algorithms Specification, 2010
[SD_6]	ISO/IEC JTC 1/SC 27 N7446 Standing Document 6 (SD6): Glossary of IT Security Terminology 2009-04-29, http://www.jtc1sc27.din.de/sce/sd6
[SMGW-PP]	Common Criteria Protection Profile for the Gateway of a Smart Metering System (BSI-CC-PP-0073), Version 1.3 – 31 March 2014
[SM-PP]	Common Criteria Protection Profile for a Security Module for Smart Metering Systems (BSI-CC-PP-0077-2013)
[PTP-A 50.8]	PTB Anforderungen PTB-A 50.8, November 2013