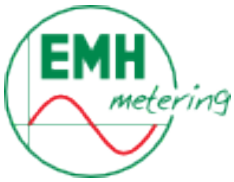


CASA 1.0 SECURITY TARGET

(CASA-ST)

VERSION: 2.13 DATE: FEBRUARY 25, 2021

EMH METERING GMBH & CO. KG
NEU-GALLINER WEG 1, 19258 GALLIN, GERMANY

History of changes

Version	Date	Author	Changes
0.80	30.08.2013	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Initial Version
1.00	29.11.2013	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Rework to fullfil the CC requirements
1.10	19.11.2013	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Rework upon the comments of the evaluator
1.20	18.12.2013	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Rework upon the comments of the evaluator
1.30	30.06.2014	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Changes according SMGW-PP Version 1.3
1.40	31.07.2014	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Changes according new design specs
1.50	06.01.2017	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Changes because of new TOE boundary & updated requirements
1.60	03.02.2017	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Rework upon the comments of the evaluator
1.70	08.02.2017	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Rework upon the comments of the evaluator
1.80	10.02.2017	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	FIA_UAU.6 refinement correction
1.81	12.09.2018	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Changes due to clarification from BSI and inconsistency removal
1.90	10.12.2018	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Changed due to OR v3
1.91	08.01.2019	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Changed due to OR v4
1.92	21.01.2019	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Changed due to OR v5
1.93	24.01.2019	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Changed due to OR v6
1.94	24.01.2019	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Rework upon the comments of the evaluator
1.95	19.03.2019	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	FAU_GEN.1/CAL event, FIA_UAU.6 CLS
1.96	30.10.2019	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Added hardware variants
1.97	14.11.2019	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Add table of public manuals
1.98	29.11.2019	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Changed due to OR v8
1.99	11.12.2019	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Changed due to certifier comments
2.00	16.12.2019	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Update AGD references

2.01	23.03.2020	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Updated references
2.10	07.07.2020	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Updated references
2.11	05.08.2020	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Updated firmware version and references
2.12	12.10.2020	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Updated firmware version and references
2.13	25.02.2021	EMH metering GmbH & Co. KG, TÜV Informationstechnik GmbH	Updated firmware version and references

Contents

List of Tables

List of Figures

1. ST introduction

1.1 Introduction

A German introduction is provided below.

In future the installation of intelligent measurement systems have to be done according to the amended Energy Act (EnWG).

The aim of using intelligent measurement systems is to ensure data protection as well as to offer a higher degree of transparency towards the consumers (end users) of their own energy consumption. The consumers have the opportunity to analyze their own consumption behavior, and to reduce their consumption and energy costs accordingly.

The Target of Evaluation (TOE) presented in this document is called "Smart Meter Gateway", “SMGW” or “Gateway” and is uniquely identified as CASA 1.0. It is the communication unit used within such an intelligent metering system and is represented by the product CASA except for the integrated Security Module and external communication interfaces.

Besides the data processing the Smart Meter Gateway offers the possibility to generate tariff rates, in order to enable network operators and consumers to control energy consumption in an intelligent way.

As personal consumption data will be recorded, processed and transmitted in the Gateway, high demands are made on data protection and data security. These security requirements were fixed in the context of the protection profile for the Smart Meter Gateway by the BSI [SMGW-PP]. In addition, the security requirements are described and amended by the Technical Guideline [TR 03109]. Further requirements result from the valid legal framework, amongst others the requirements of the PTB with the [PTB A50.8].

The main functionality of the Gateway is the reception, the verification and the storage of measured values and status of the connected meters as well as the processing and the transfer of these measurements and status values. The transmission is done via the remote connection to authorized external entities, as for example, the metering point operators.

Additionally the Gateway realizes functions for the consumer and the service technician, to enable them the retrieval of consumption data or system information via the local interface HAN (HAN = Home Area Network).

For controllable systems connected to the CLS interface (CLS = Controllable Local System), such as for example a control box, the Gateway acts as a forwarding entity. The transfer of this data to and from the Smart Meter Gateway is done via encrypted communication channels.

According to [SMGW-PP], the Smart Meter Gateway performs as a firewall and separates the connected networks from each other. The gateway as a decentralized storage for personal measured values ensures data protection for the consumer.

Im Zuge der Installation intelligenter Messsysteme müssen diese künftig entsprechend des novellierten Energiewirtschaftsgesetzes (EnWG) eingesetzt werden.

Ziel des Einsatzes intelligenter Messsysteme ist neben dem Datenschutz auch, dem Kunden (Letztverbraucher) eine höhere Transparenz über den eigenen Energieverbrauch zu ermöglichen. Er erhält so die Chance, das eigene Verbrauchsverhalten zu analysieren und entsprechend den Verbrauch und damit die Energiekosten senken zu können.

Der in diesem Dokument vorgestellte Evaluationsgegenstand (Target of Evaluation (TOE)) CASA 1.0 wird repräsentiert durch das Gerät CASA mit Ausnahme des integrierten Sicherheitsmoduls und der externen Kommunikationsschnittstellen. Im Folgenden wird der Evaluationsgegenstand als “Smart Meter Gateway, “SMGW” oder “Gateway” bezeichnet. Dieses stellt die Kommunikationseinheit innerhalb eines solchen intelligenten Messsystems dar.

Das Smart Meter Gateway ermöglicht neben der Messwertverarbeitung auch die Bildung von Tarifmodellen, damit die Netzbetreiber und Letztverbraucher den Energieverbrauch intelligent gestalten können.

Da personenbezogene Verbrauchsdaten im Gateway erfasst, bearbeitet und übertragen werden, sind hohe Anforderungen an den Datenschutz und die Datensicherheit zu stellen. Diese Sicherheitsanforderungen wurden im Rahmen des Schutzprofils für das Smart Meter Gateway [SMGW-PP] vom BSI erstellt und werden zusätzlich durch die Technische Richtlinie [TR 03109] beschrieben und ergänzt. Weitere Anforderungen ergeben sich aus dem gültigen Rechtsrahmen, unter Anderem den Anforderungen der PTB mit der [PTB A50.8].

Die Hauptfunktionalität des Gateways besteht im Empfang, der Überprüfung und der Speicherung von Mess- und Statuswerten angeschlossener Zähler sowie der Verarbeitung und Versendung dieser Mess- und Statuswerte. Der Versand erfolgt dabei über die Fernverbindung an berechtigte externe Marktteilnehmer, zu denen beispielsweise die Messstellenbetreiber gehören.

Zusätzlich realisiert das Gateway Funktionen für den Letztverbraucher und den Service-Techniker, damit diese über die lokale HAN-Schnittstelle (HAN = Home Area Network) Verbrauchsdaten bzw. Systeminformationen abrufen können.

Für die an der CLS-Schnittstelle (CLS = Controllable Local Systems) angeschlossenen steuerbaren Systeme, wie beispielsweise eine Steuerbox, fungiert das Gateway als weiterleitende Instanz. Die Übertragung dieser Daten von und zum Smart Meter Gateway erfolgt dabei über verschlüsselte Kommunikationskanäle.

Gemäß [SMGW-PP] erfüllt das Smart Meter Gateway die Aufgaben einer Firewall und separiert die angebundenen Netze voneinander. Als dezentraler Speicher für personenbezogene Messwerte stellt das Gateway den Datenschutz für den Letztverbraucher sicher.

1.2 ST Reference

Title	CASA 1.0 Security Target (CASA-ST)
Version	2.13
Date	February 25, 2021
Author	EMH metering GmbH & Co. KG TÜV Informationstechnik GmbH
Certification Authority	Bundesamt für Sicherheit in der Informationstechnik Federal Office for Information Security, Germany
Certification-ID	BSI-DSC-CC-0919v2
CC-Version	3.1 Revision 5
Evaluation Assurance Level	EAL 4 augmented by AVA_VAN.5 and ALC_FLR.2
Keywords	Smart Metering, Security Target, Meter, Gateway, ST
PP Conformance	This ST claims strict conformance to [SMGW-PP] with the exception of using the updated version [SM-PP] of the Security Module Protection Profile instead of BSI-CC-PP-0077-2013 referenced by the [SMGW-PP].

1.3 TOE Reference

The TOE is uniquely identified as follows:

TOE Identification	CASA 1.0
TOE Software Version	30100000__X026e
TOE Hardware Version	10 301 / 10 302 / 10 303 / 10 304[1]
TOE Developer	EMH metering GmbH & Co. KG

Please note that the TOE is part of the product CASA. In particular the TOE comprises all hard- and software components including the casing of CASA but excluding the Security Module and hardware external communication interfaces which are physically integrated into CASA. Details of the exact TOE hardware boundary are specified in chapter 1.5.8. It should be noted that from a purely functional perspective the TOE comprises the whole gateway except the Security Module, i.e. for the gateway software, which is responsible for establishing authenticated and integrity-protected communications channels, having the hardware external communication interfaces inside or outside the TOE boundary make no difference.

[1] Please note that this is a set of four alternative Hardware Versions of one TOE configuration, denoted by the forward slash separator '/'; each variant describes the application of specific form, fit and function equivalent hardware components. Since the test standard for those components is equal, no security issue arises using an alternative Hardware Version

The customer will receive public manuals with the TOE as listed in Table 1.

Attribute	Value
Document Title	CASA 1.0 – Benutzerhandbuch für Letztverbraucher
Filename	CASA-PHB-LV-DE-1.24.pdf
sha256 Hash	25f244a5a78950eeab32df48dce26a913ba50474e712b0c5392b2b5838790adf
Document Title	CASA 1.0 – Installations- und Inbetriebnahmehandbuch für Service-Techniker und Gateway-Administratoren
Filename	CASA-PHB-ST-GWA-DE-1.24.pdf
sha256 Hash	ffd944d191236bf481a6e814b315f937b630c7ecaae191b7c8e608c7dbeac248
Document Title	CASA 1.0 – SMGw-Schnittstellenbeschreibung (CASA API)
Filename	CASA_API-SMGW_v1.30_2020-06-11_attachment.pdf
sha256 Hash	d555771712e48ba45869719e9a73ec62a86dd4eceedae5e9be35119bfffa426c

Table 1: Public manuals that are available to the customer

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 Security Target 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[2]	
Consumer	End user of electricity, gas, water or heat. The consumer can also generate energy using a Distributed Energy Resource.	[CEN]

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

Term	Definition	Source (if any)
Gateway Smart Meter Gateway (SMGW)[3]	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 focusses 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 ST 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 kinds of commodities.	[CEN], adopted

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

Term	Definition	Source (if any)
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[4] (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

[4]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[5].

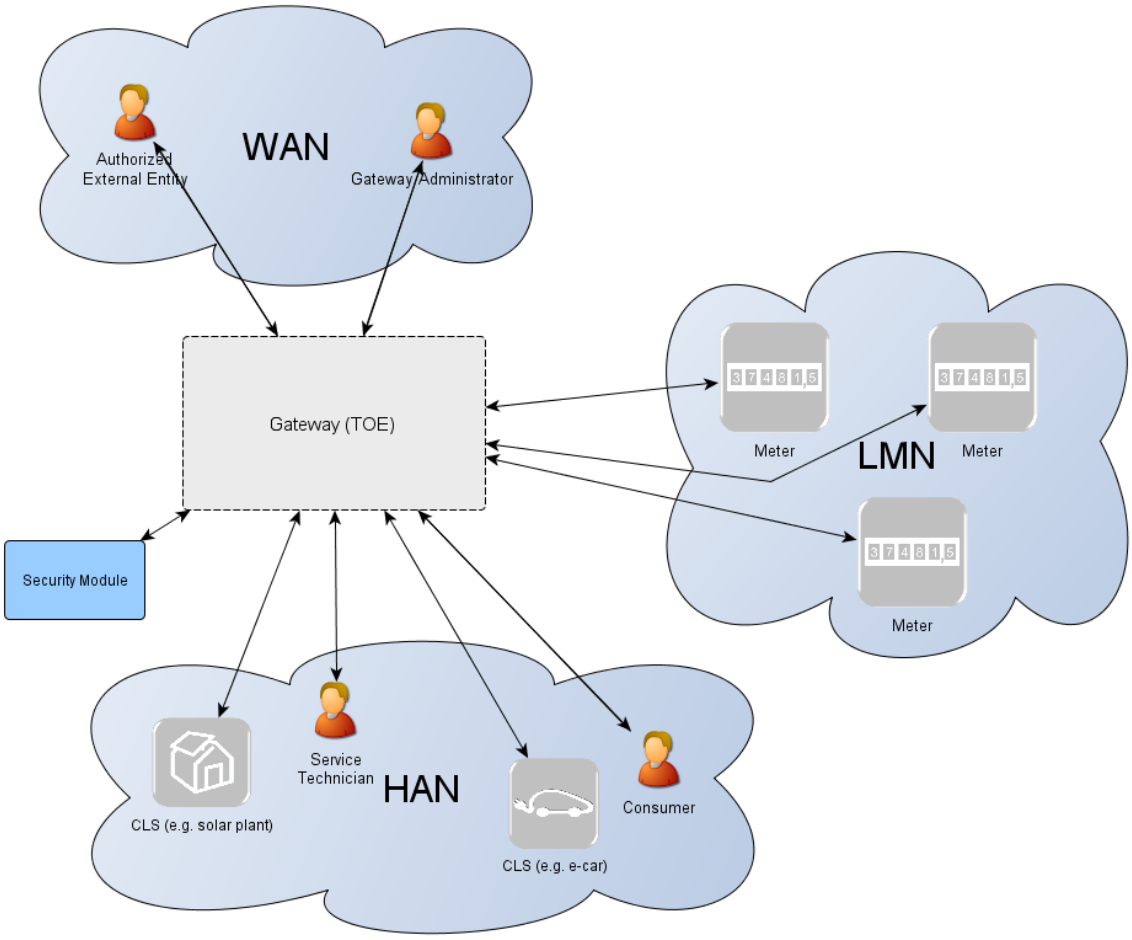


Figure 1: The TOE and its direct environment[6]

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:

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

[6] taken from [SMGW-PP, Figure 1, p. 11]

- 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[7] the information will be encrypted and signed using the services of a Security Module. The Gateway features a mandatory user interface, enabling authorised consumers to access the data relevant to them.
- The **Meter** itself records the consumption or production of one or more commodities (e.g. electricity, gas, water, heat) and submits those records in defined intervals to the Gateway. The Meter Data has to be signed and encrypted before transfer in order to ensure its confidentiality, authenticity and integrity. The Meter is comparable to a classical meter[8] and has comparable security requirements; it will be sealed as classical meters are today according to the regulations of the calibration authority [PTB A50.7]. The Meter further supports the encryption and integrity protection of its connection to the Gateway[9].
- The Gateway utilizes 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 utilize 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. Detailed information regarding the logical and physical interfaces of the TOE is provided in subsection 1.5.7 and subsection 1.5.8.

Please note that the arrows of the interfaces within the Smart Metering System as shown in Figure 2 indicate the initialization of the information flow. In fact, the following chapters of this ST will place dedicated requirements on the way an information flow can be initiated[10].

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

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

[9] More information on the requirements that the Meter shall fulfill to communicate with the TOE is provided in subsection 1.5.3.

[10] 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.

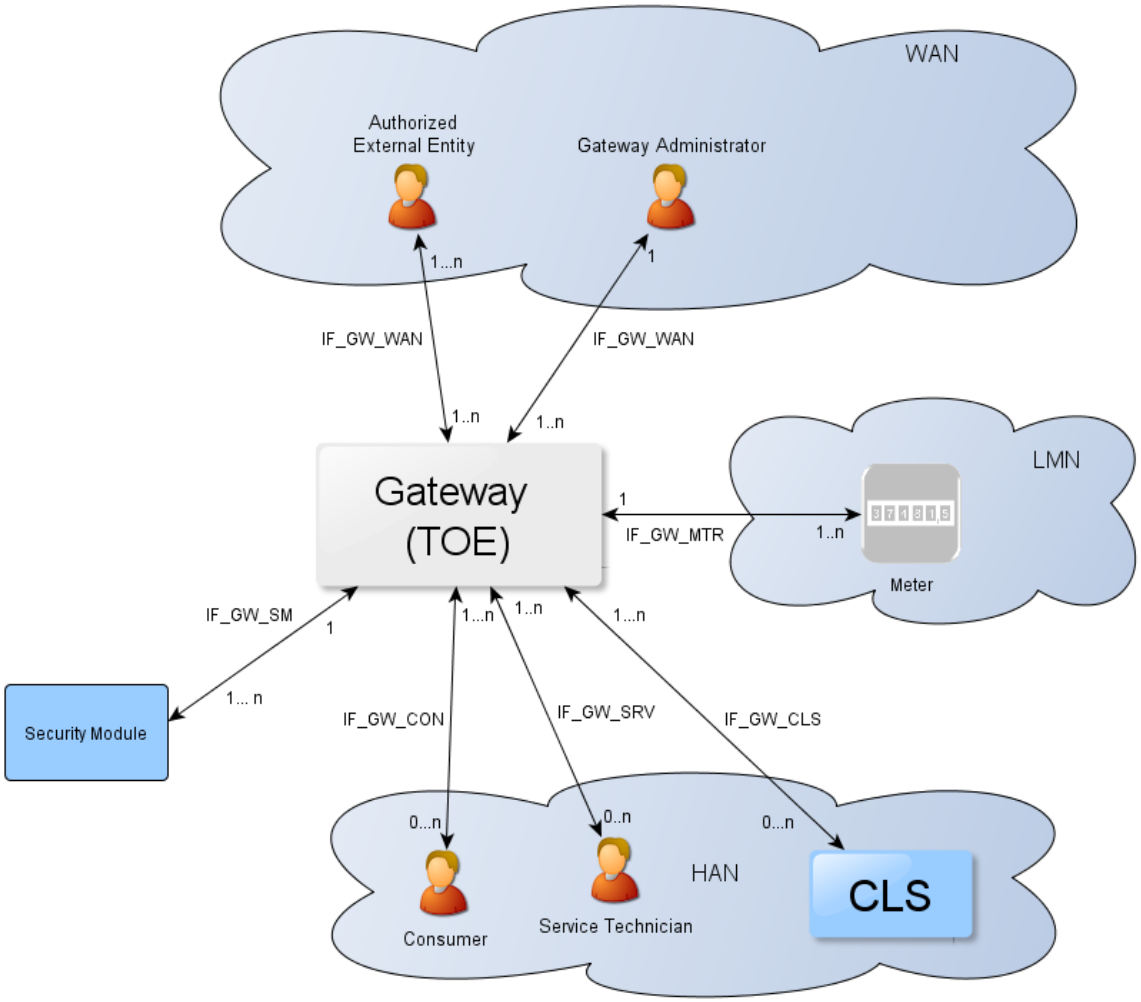


Figure 2: The logical interfaces of the TOE[11]

1.5.3 Requirements on the operational environment of the TOE

For a secure operation of the TOE a Security Module that is Common Criteria certified in conformance to [SM-PP] is physically integrated into the CASA. Please note, that the Security Module is not part of the TOE.

Other requirements on the operational environment do not compromise the security functionality of the TOE but should be considered to ensure the availability of all services provided by the TOE.

Therefore a power supply providing the necessary voltages and currents, a GSM modem providing a FAKRA D, a wM-Bus module providing a FAKRA C and a RS485 converter providing a RJ12 interface are physically integrated into the CASA and attached to the TOE.

Wired attached Meters located in the LMN network shall provide an EIA/RS-485 interface and support communication via COSEM objects using SML. Further those Meters shall be able to communicate with the TOE using TLS via HDLC. Wirelessly attached Meters shall provide a wM-Bus compatible transmitter for a unidirectional communication and in addition a wM-Bus compatible receiver, if bidirectional communication should be possible.

[11] taken from [SMGW-PP, Figure 2, p. 12]

To receive Meter Data the consumer shall provide a device that is attached to the TOE via the IF_GW_CON interface. This device shall provide an Ethernet-interface and support the protocols HTTPS and TCP/IP. Further the TOE needs a direct connection to the internet without any proxy server between itself and the Gateway Administrator via the IF_GW_WAN interface. Therefore the TOE implements GSM and an Ethernet interface. To use the GSM interface a SIM card is required. In order to send billing relevant data to authorized External Entities the internet connection must provide at least GPRS CS-3 or CS-4 speed. The GPRS speed is also sufficient to enable the Gateway Administrator to manage the TOE as well as to provide firmware updates. More information on communication protocols used within this interface is provided in [TR 03109-1]. In addition the Gateway Administrator shall provide a reliable time source that is used by the TOE to update its local time. More information on the requirements for the reliable time source is provided in [TR 03109-1].

1.5.4 TOE description

The Smart Metering Gateway (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[12] 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[13].

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 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)

[12] 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.

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

- **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.

1.5.6.1 Handling of Meter Data[14]

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. Further Processing Profiles are used to allocate and connect Meter located in the LMN to the SMGW. More details on the Processing Profiles can be found in [TR 03109-1].
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.

The Gateway shall accept data (e.g. configuration data, firmware updates) from a correspondingly authorised Gateway Administrator 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

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

- 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[15],
- 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 a billing process that ensures that the value of the consumed amount of a certain commodity (and only the used amount) is transmitted[16],
- preserve the integrity of the system components and their configurations.

The TOE offers a local interface to the consumer (see also IF_GW_CON in Figure 2) and allows the consumer to obtain information via this interface. This information comprises the billing-relevant data (to allow the consumer to verify an invoice) and information about which Meter Data has been and will be sent to which external entity. The TOE ensures that the communication to the consumer is protected by using TLS and ensures that consumers only get read-only access to their own data.

1.5.6.2 Confidentiality protection

The TOE protects data from unauthorised disclosure

- while received from a Meter via the LMN,
- while received from the Gateway 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).

1.5.6.3 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.

[15]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.

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

- 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.

1.5.6.4 Information flow control and firewall

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

- only the Gateway may establish a connection to an external entity in the WAN[17]; 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 offers a wake-up service that allows external entities in the WAN to trigger a connection establishment by the Gateway,
- connections are allowed to pre-configured addresses only,
- only cryptographically-protected (i.e. encrypted, integrity protected and mutually authenticated) connections are possible.

These functionalities

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

[17] 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.

The communication flows that are enforced by the Gateway between parties in the HAN, LMN and WAN are summarized in the following table[18]:

Source (1st column) Destination (1st row)	**WAN**	**LMN**	**HAN**
WAN	– (see following list)	No connection establishment allowed	No connection establishment allowed
LMN	No connection establishment allowed	– (see following list)	No connection establishment allowed
HAN	Connection establishment is allowed to trustworthy, preconfigured endpoints and via an encrypted channel only[19]	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.

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

1. The Gateway accepts the submission of Meter Data from the LMN,
2. the Gateway offers a wake-up service at the WAN side as described in chapter 1.5.6.5,
3. the Gateway offers a user interface to the HAN that allows CLS or consumers to connect to the Gateway in order to read relevant information.

[18] 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.

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

1.5.6.5 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)[20].
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, the Gateway keeps existing connections to external entities open (please refer to [TR 03109-3] for more details) and offers a so called wake-up service.
The Gateway is able to receive a wake-up message that is signed by the Gateway Administrator. The following steps are taken:

1. The Gateway verifies the wake-up packet. This comprises
   (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 [TR 03109-1, “Wake-Up-Service”].

1.5.6.6 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 TOE submits only a minimum amount of data to external entities and therewith leaves the scope of control to the consumer. The mechanisms “encryption” and “pseudonymisation” ensure that the data can only be read by the intended recipient and only contains an association with the identity of the Meter if this is necessary.
On the other hand, the TOE provides the consumer with transparent information about the information flows that happen with their data. In order to achieve this, the TOE implements a consumer log that

[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.

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 via HAN-certificates[21] or via username and password. 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 keeps 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 provides detailed and complete reporting in the consumer log of each security and privacy-relevant configuration setting. Additional to device specific configuration settings the consumer log contains the parameters of each Processing Profile. The consumer log contains the configured addresses for internal and external entities including the CLS.

Audit Log and Monitoring

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

1.5.6.7 Management of Security Functions

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

Further, it is defined that only authorised Gateway Administrators are 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 is only possible from the WAN side interface.

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

1.5.6.8 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.

1.5.7 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:

[21] see [TR 03109-1] for more details

Interface Name	Description
IF_GW_CON	Via this interface the Gateway provides the consumer[22] 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.[23]
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

1.5.8 TOE physical boundary

The TOE comprises the hardware and software of the Gateway CASA 1.0 accompanied by its guidance documentation. The design of the product follows the design proposal of [SMGW-PP, chapter 1.4.5.2] as depicted in Figure 3 where the TOE boundary is not identical to the device's casing. The TOE merely comprises the security functions. Additionally integrated into the product are non-TSF interfaces as well as the Security Module.

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

[23] 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.

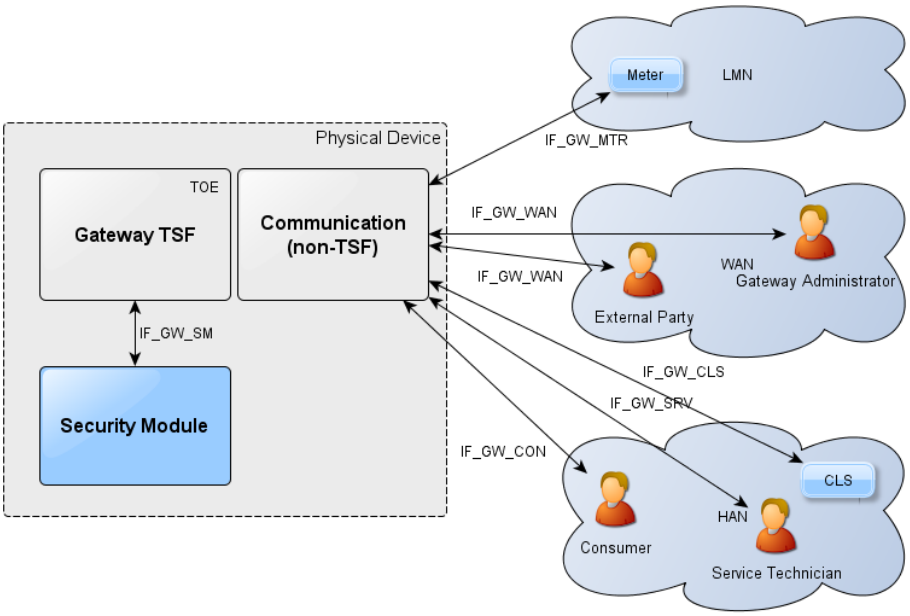


Figure 3: General design of the product[24]

The hardware and software parts as well as the boundary of the TOE are described in the following subsection.

1.5.8.1 Overview of the TOE hardware

Figure 4 provides an overview about the casing of the TOE. In particular, the figure shows all external interfaces of the CASA.[25] Figure 5 shows the CASA equipped with an optional HAN module with RJ-45 interface.

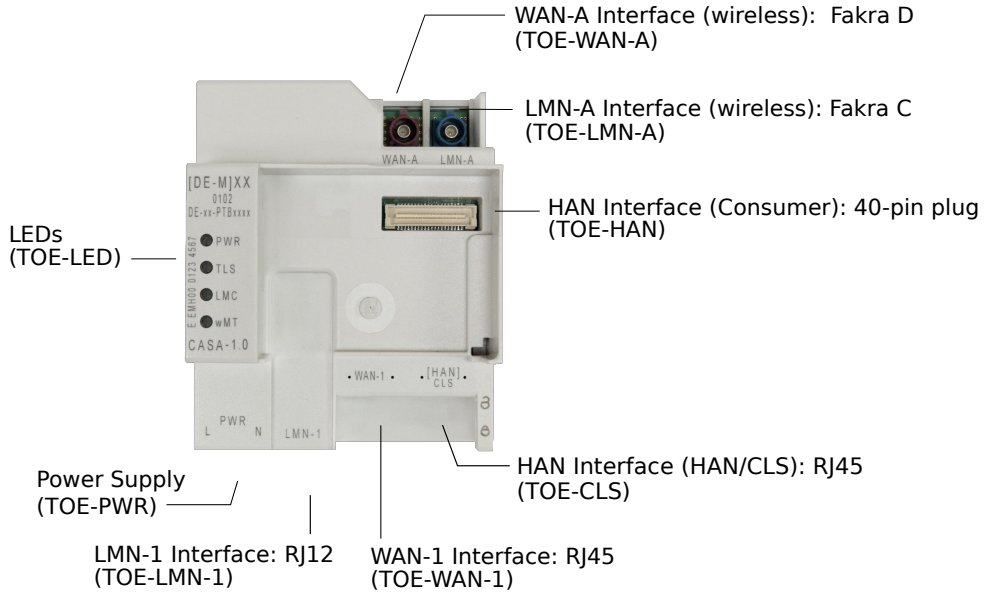


Figure 4: Casing of the TOE

[24] taken from [SMGW-PP, Figure 3, p. 15]

[25] Please note that the external interfaces of the CASA are not identical to the interfaces of the TOE.

Figure 5: Casing of the TOE with optional HAN module

Figure 6 shows the hardware parts of CASA as well as the TOE boundary. The light green area denotes hardware parts which are included in the TOE. Specifically, the independent Power Supply Circuit Board containing the Power Supply, the RS485 converter, the wM-Bus module as well as the GSM module is physically integrated into the gateway but excluded from the TOE. Further, the Security Module is integrated into the gateway but excluded from the TOE. Please note, that all TSF-data which is exchanged across the TOE boundary is encrypted and integrity-protected.

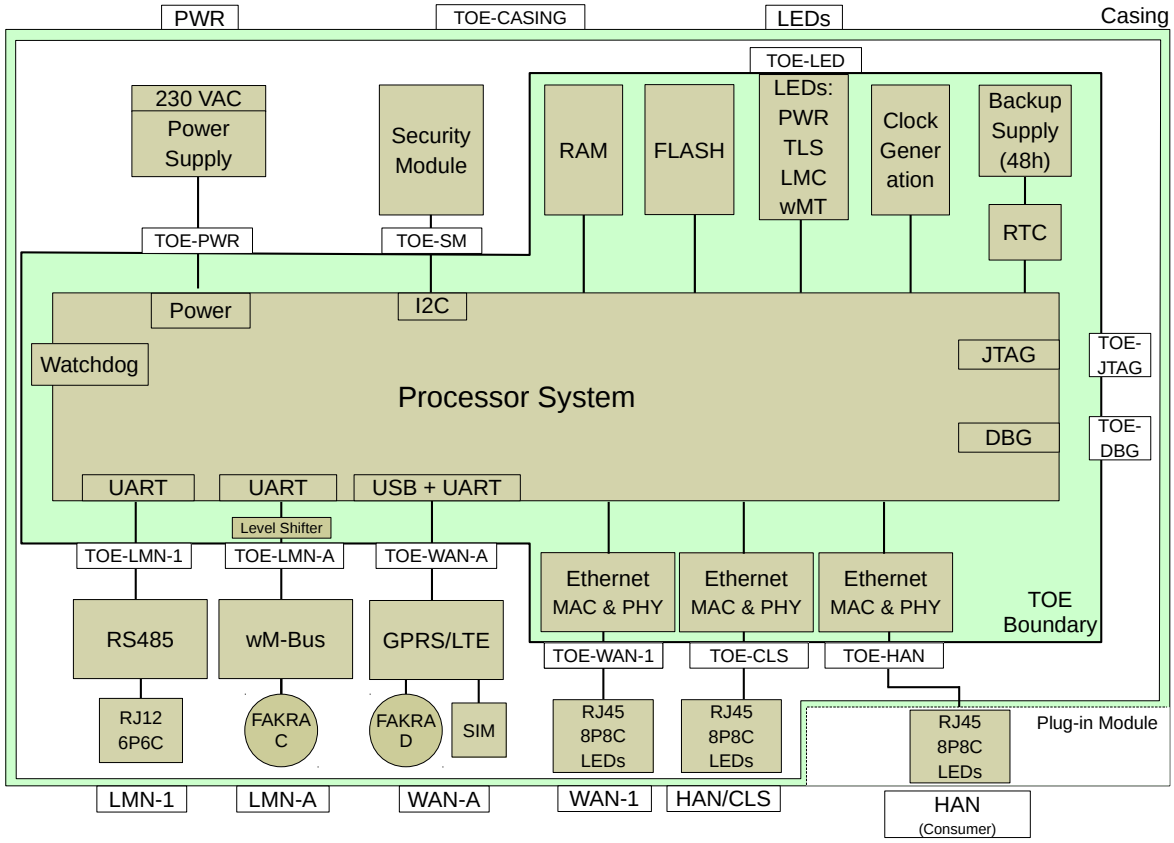


Figure 6: The hardware parts of the TOE

The hardware components shown in Figure 6 are briefly described below:

Power Supply

This component supplies all other components of CASA with voltage providing the correct powersequencing. It provides the external interface Power Supply (PWR) (cf. Figure 4).

Security Module

Mainly the TOE uses the functionality of the Security Module for cryptographic support. The TOE name of the Security Module is "TCOS Smart Meter Security Module Version 1.0 Release 2/P60C144PVE", certified as BSI-DSZ-CC-0957-V2-2016. For more information please refer to subsection 1.5.9.

RAM

This component provides random access memory used by the Processor System.

FLASH

This component provides non-volatile storage used for code and data.

LEDs

The TOE comprises four LEDs which are located on the front side of the SMGW casing indicating the status of the TOE.

Clock Generation

This component provides clock signals for the Clock System inside of the Processor and other TOE components.

Backup Supply (RTC)

This component supplies the Real Time Clock (RTC) with voltage for a particular amount of time if the component power supply is down. Therefore it is ensured that the RTC keeps running within this timeframe.

RTC

The Real Time Clock (RTC) of the TOE is used to synchronize the internal system time of the TOE after a power cut. During the operation of the TOE the RTC is adjusted using the internal system time of the TOE, if the internal system time corresponds to the reliable time source provided by the Gateway Administrator.

Watchdog

This component monitors the operation of the TOE and performs a reboot of the TOE if necessary.

Processor System

The Processor System as part of the CPU comprises the following main components:

- Clock System

  The Clock System uses the clock provided by the Clock Generation to provide the clock to the Processor System.

- JTAG- and Debug-Interface

  The JTAG- and Debug-Interface is used for testing during production and to import the initial software into the SMGW and will be deactivated afterwards.

IF_GW_MTR

The logical interface IF_GW_MTR is realized by the following two physical components:

- LMN-1 (RS-485)

  This component provides the external interface LMN-1 (cf. Figure 4) and hence, enables a wired connection between the TOE and Meters located in the LMN. Therefore the gateway provides an RJ12-Socket with 6P6C connected to the TOE interface TOE-LMN-1. Further this interface is used to supply some of the Meters using this interface with voltage.

- LMN-A (wM-Bus)

  This component provides the external interface LMN-A (cf. Figure 4) and hence, enables the communication between the TOE and Meters located in the LMN via wireless M-Bus. Therefore the gateway provides a FAKRA C-Socket connected to the TOE interface TOE-LMN-A and an LED that displays the connection status (cf. wMT LED in Figure 4).

IF_GW_WAN

The logical interface IF_GW_WAN is realized by the following two physical components:

- WAN-A (GPRS/LTE)

  This component enables the wireless communication between the TOE and external entities located in the WAN. Therefore the gateway provides a FAKRA D-Socket and a SIM card slot connected via a GPRS/LTE module to the TOE interface TOE-WAN-A. This component implements the external interface WAN-A (cf. Figure 4).

- WAN-1 (Ethernet)

  This component implements the external interface WAN-1 (cf. Figure 4) and hence, enables a wired connection between the TOE and external entities located in the WAN. Therefore the gateway provides an RJ45-Socket with 8P8C which is connected to the TOE interface TOE-WAN-1. After the installation and start of operation (cf. subsection 1.5.10) the RJ45-Socket is located inside the sealed cabinet where the SMGW is installed.

IF_GW_CLS
The logical interface IF_GW_CLS is realized by the physical interface HAN/CLS (Ethernet) which is an RJ45-Socket with 8P8C. After the installation and start of operation (cf. subsection 1.5.10) this socket is located inside the sealed cabinet enclosing the SMGW.
IF_GW_CON
The logical interface IF_GW_CON is realized by the physical interface HAN (Ethernet) which is a pin header. The pin header is used to connect an optional HAN module which may provide an RJ45-Socket with 8P8C or may be equipped with other non-TOE HAN components to provide an authenticated user the ability to connect a display or another device to get access to the consumer log (HAN Interface (Consumer), cf. Figure 4).
IF_GW_SRV
The logical interface IF_GW_SRV is realized by both, the HAN/CLS and the HAN (Consumer) physical interfaces to allow Service Technicians to access the TOE.

1.5.8.2 Overview of the TOE software

Figure 7 provides an overview of the software parts of CASA:

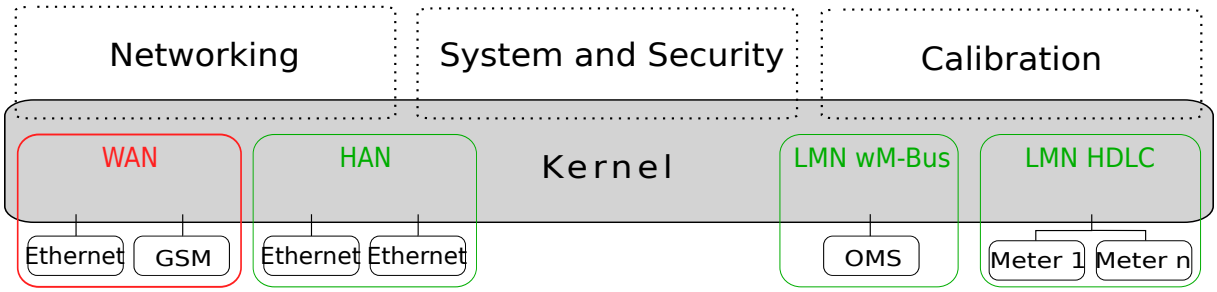


Figure 7: The software parts of the TOE

A brief description of all software parts represented in the figure above is provided below:
Networking
The networking part of the software provides the functionality of establishing secure, authenticated and integrity-protected communication channels via TLS with communication partners in the WAN and HAN. It is further responsible for providing the interfaces to the consumers, the Gateway Administrator and the Service Technician.
System and Security
The system and security part of the software is responsible for the secure initialization of the TOE and provides the audit record generation, secure file storage and self-test facilities to ensure the secure operation. It also manages all profiles and settings as well as the access to the Security Module.
Calibration
The calibration part of the software is responsible for handling Meter data. That includes correctly gathering, tariffing and storing all Meter data from the LMN as well as dispatching correctly aggregated data to authorized external entities.
Kernel
The kernel provides several operating system functions, e.g. for the required hardware interfaces.

1.5.9 The cryptography of the TOE and its Security Module

Parts of the cryptographic functionality used in the aforementioned 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 CASA 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**
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 • random number generation • digital signature verification and 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 (in case of TLS connection) • 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

Aspect	TOE	Security Module

Table 5: Cryptographic support of the TOE and its Security Module

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 [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 8:

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.
   (c) If a unidirectional communication is performed between the Meter and the Gateway the Meter Data is encrypted using a symmetric algorithm (according to [TR 03109-3]) and facilitating a defined data structure to ensure the authenticity and confidentiality.
3. The authenticity and integrity of the Meter Data is verified by the Gateway
4. If (and only if) authenticity and integrity have been verified successfully the Meter Data is further processed by the Gateway according to the rules in the Processing Profile else the cryptographic information flow will be cancelled.
5. The processed Meter Data is encrypted and integrity protected using CMS (according to [TR 03109-1-I]) for the final recipient of the data[26].
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.

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

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

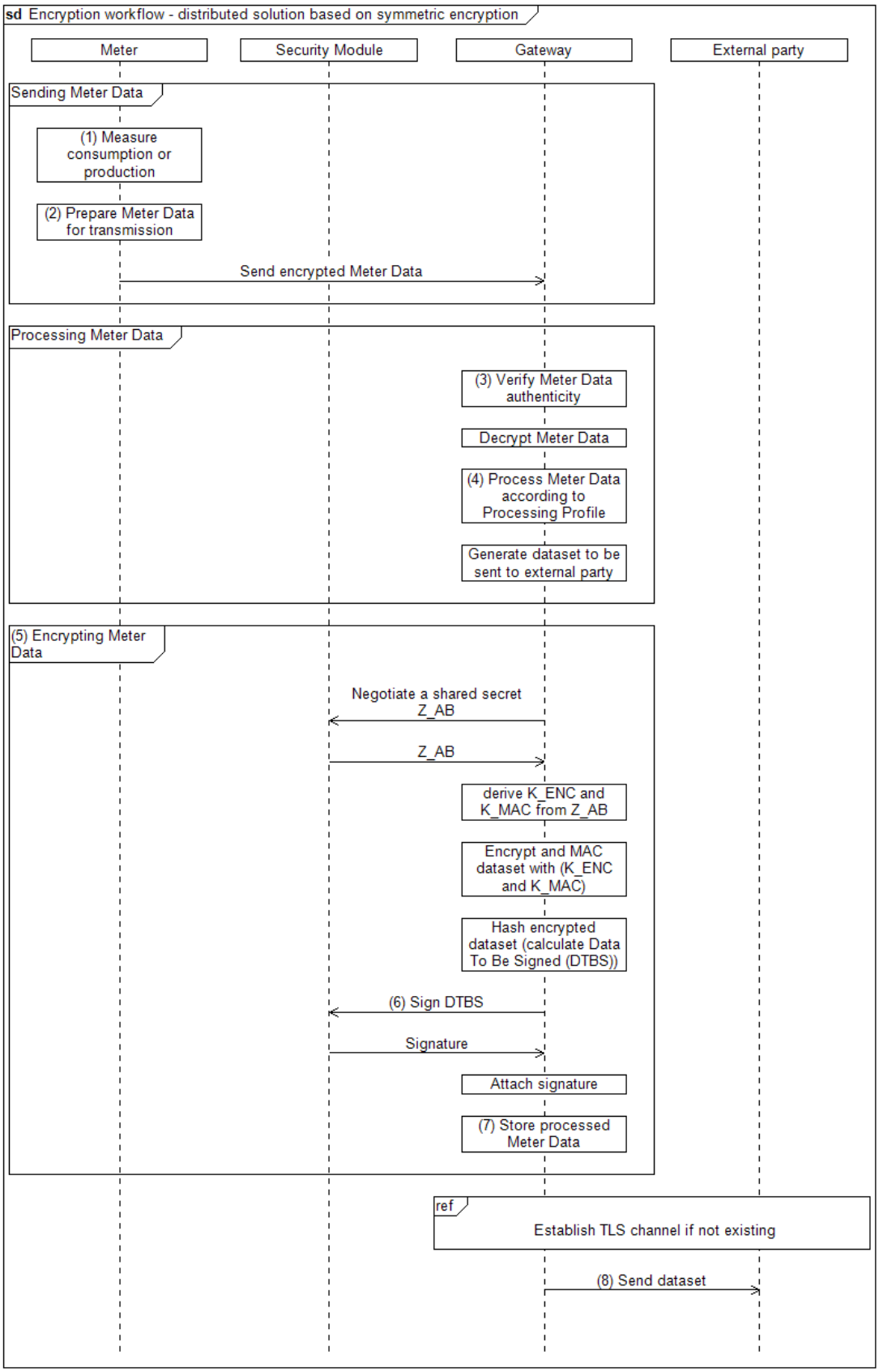


Figure 8: Cryptographic information flow for distributed Meter and Gateway

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 [TR 03109-1-VI].
The certified configuration of the TOE will be established after phase "Personalization". It is ensured that previous phases are performed by trusted personnel in secure environments.

2. Conformance Claims

2.1 CC Conformance Claims

This ST has been developed using Version 3.1 Revision 5 of Common Criteria [CC]. This ST is [CC] part 2 extended due to the use of FPR_CON.1. This ST is [CC] part 3 conformant; 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] with the exception of using the updated version [SM-PP] of the Security Module Protection Profile instead of BSI-CC-PP-0077-2013 referenced by the [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 claims strict conformance to the Gateway PP and no other security requirements are added. All assignments and selections of the security functional requirements are done in the Gateway PP [SMGW-PP] and in this security target section 6.1.

The relied upon Security Module is the only exception as it is certified using the updated version BSI-CC-PP-0077-V2 of the Protection Profile for the Security Module of a Smart-Meter-Gateway (Security Module PP) ([SM-PP]) instead of the version BSI-CC-PP-0077-2013 referenced by the [SMGW-PP].

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 Meters and Gateway. Those roles have been defined for the use in this Security Target. It is possible that a party implements more than one role in practice.

Role	Description
Consumer	The authorised individual or organization that "owns" the Meter Data. In most cases this will be tenants or house owners consuming electricity, water, gas or further commodities. However, it is also possible that the consumer produces or stores energy (e.g. with their own solar plant).
Gateway Administrator	Authority that installs, configures, monitors, and controls the Smart Meter Gateway.
Service Technician	The authorised individual that is responsible for diagnostic purposes.
Authorised External Entity / User	Human or IT entity possibly interacting with the TOE from outside of the TOE boundary. In the context of this ST the term user or external entity serve as a hypernym for all entities mentioned before.

Table 6: Roles used in the Security Target

3.2 Assets

The following tables introduce the relevant assets for this Security Target. 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)

Asset	Description	Need for Protection
System log data	Log data from the • system log.	• Integrity • Confidentiality (only authorised SMGW administrators and Service technicians may read the log data)
Consumer log data	Log data from the • consumer log.	• Integrity • Confidentiality (only authorised Consumers may read the log data)
Calibration log data	Log data from the • calibration log.	• Integrity • Confidentiality (only authorised SMGW administrators may read the log data)
Consumption Data	Billing-relevant part of Meter Data. Please note that the term Consumption Data implicitly includes Production Data.	• Integrity and authenticity (comparable to the classical meter and its security requirements) • Confidentiality (due to privacy concerns)
Status Data	Grid status data, subset of Meter Data that is not billing-relevant[27].	• 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 / User Data	The term Data is used as a hypernym for Meter Data and Supplementary Data.	• According to their specific need

[27] 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
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":

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
Firmware (secondary asset)	The firmware of the TOE	• Integrity • 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 table lists assumptions about the environment of the components in this threat model that need to be taken into account in order to ensure a secure operation.

A.ExternalPrivacy	It is assumed that authorised and authenticated external entities receiving any kind of privacy-relevant data or billing-relevant data and the applications that they operate are trustworthy (in the context of the data that they receive) and do not perform unauthorised analyses of this data with respect to the corresponding consumer(s).
A.TrustedAdmins	It is assumed that the Gateway Administrator and the Service Technician are trustworthy and well-trained.
A.PhysicalProtection	It is assumed that the TOE is installed in a non-public environment within the premises of the consumer which provides a basic level of physical protection. This protection covers the TOE, the Meter(s) that the TOE communicates with and the communication channel between the TOE and its Security Module.
A.ProcessProfile	The Processing Profiles that are used when handling data are assumed to be trustworthy and correct.
A.Update	It is assumed that firmware updates for the Gateway that can be provided by an authorised external entity have undergone a certification process according to this Security Target before they are issued and can therefore be assumed to be correctly implemented. It is further assumed that the external entity that is authorised to provide the update is trustworthy and will not introduce any malware into a firmware update.
A.Network	It is assumed that • a WAN network connection with a sufficient reliability and bandwidth for the individual situation is available, • one or more trustworthy sources for an update of the system time are available in the WAN, • the Gateway is the only communication gateway for Meters in the LMN[28], • 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 [TR 03109-3] and brought into the Gateway in a secure way by the Gateway Administrator.

[28] 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.

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.

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

3.4 Threats

The following sections identify the threats that are posed against the assets handled by the Smart Meter 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, or 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 Meter or 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 definition of the following threats acknowledges that the local attacker (facilitating physical access) has less motivation for an attack than a remote attacker.
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 [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 devices within the LAN to external entities within the WAN and shall provide firewall functionality in order to protect the devices of the LMN and HAN (as long as they use the Gateway) and itself against threats from the WAN side.

The firewall:

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

O.SeparateIF

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

Application Note 3:

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

O.Conceal

To protect the privacy of its consumers, the TOE shall conceal the communication with external entities in the WAN in order to ensure that no privacy-relevant information may be obtained by analysing the frequency, load, size or the absence of external communication.[29]

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

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[30],
- the TOE shall verify the integrity and authenticity of the data received from a Meter before handling it further,
- the TOE shall process the data according to the definition in the corresponding Processing Profile,
- the TOE shall encrypt the processed Meter Data for the final recipient, sign the data and
- deliver the encrypted data to authorised external entities as defined in the corresponding Processing Profiles facilitating an encrypted channel,
- the TOE shall store processed Meter Data if an external entity cannot be reached and re-try to send 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.

[30] It is acknowledged that the implementation of a secure channel between the Meter and the Gateway is a security function of both units. The TOE as defined in this Security Target only has a limited possibility to secure this communication as both sides have to sign responsible for the quality of a cryptographic connection.

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.[31].

In addition the TOE shall generate the required keys utilising the services of its Security Module[32], ensure that the keys are only used for an acceptable amount of time and destroy ephemeral[33] 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 not longer needed to ensure that it is no longer available via the external interfaces of the TOE
- 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)[34],
- make any physical manipulation within the scope of the intended environment detectable for the consumer and Gateway Administrator.

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

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

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

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

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

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

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

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

1. A system log of relevant events in order to allow an authorised Gateway Administrator or an authorised Service Technician to analyse the status of the TOE. The TOE shall also analyse the system log automatically for a cumulation of security relevant events.

2. A consumer log that contains information about the information flows that have been initiated to the WAN and information about the Processing Profiles causing this information flow as well as the billing-relevant information and information about the system status (including relevant error messages).

3. A calibration log that provides the Gateway Administrator with a possibility to review calibration relevant events.

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

1. Access to the information in the system log shall only be allowed for an authorised Gateway Administrator via IF_GW_WAN or for an authorised Service Technician via IF_GW_SRV.

2. Access to the information in the consumer log shall only be allowed for an authorised consumer via the IF_GW_CON interface of the TOE and via a secured (i.e. confidentiality and integrity protected) connection. The consumer shall only have access to their own information.

3. Read-only access to the information in the calibration log shall only be allowed for an authorised Gateway Administrator via the WAN interface of the TOE.

The system log overwrites the oldest events in case that the audit trail gets full. For the consumer log the TOE ensures that a sufficient amount of events is available (in order to allow a consumer to verify an invoice) but may overwrite older events in case that the audit trail gets full.

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

O.Access	The TOE shall control the access of external entities in WAN, HAN or LMN to any information that is sent to, from or via the TOE via its external interfaces[35] Access control shall depend on the destination interface that is used to send that information.

4.2 Security objectives for the operational environment

OE.ExternalPrivacy	Authorised and authenticated external entities receiving any kind of private or billing-relevant data shall be trustworthy and shall not perform unauthorised analyses of these data with respect to the corresponding consumer(s).
OE.TrustedAdmins	The Gateway Administrator and the Service Technician shall be trustworthy and well-trained.
OE.PhysicalProtection	The TOE shall be installed in a non-public environment within the premises of the consumer that provides a basic level of physical protection. This protection shall cover the TOE, the Meters that the TOE communicates with and the communication channel between the TOE and its Security 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 Security Target before they are issued to show that the update is implemented correctly. The external entity that is authorised to provide the update shall be trustworthy and ensure that no malware is introduced via a firmware update.

[35] 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.

OE.Network It shall be ensured that

- a WAN network connection with a sufficient reliability and bandwidth for the individual situation is available,
- one or more trustworthy sources for an update of the system time are available in the WAN,
- the Gateway is the only communication gateway for Meters in the LMN,
- if devices in the HAN have a separate connection to parties in the WAN (beside the Gateway) this connection is appropriately protected.

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

4.3 Security 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 Meter. **O.Crypt** defines the required cryptographic functionality. Both objectives together ensure that the communication between the Meter and the TOE cannot be disclosed.

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

4.3.2.7 T.Infrastructure

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

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

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

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

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

4.3.2.8 T.ResidualData

The threat **T.ResidualData** is mitigated by the security objective **O.Protect** as this security objective defines that the TOE shall delete information as soon as it is no longer used. Assuming that a TOE follows this requirement an attacker can not 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

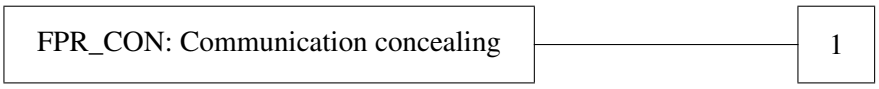
5.1 Communication concealing (FPR_CON)

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 ST:

Class FAU: Security Audit	
FAU_ARP.1/SYS	Security alarms for System Log
FAU_GEN.1/SYS	Audit data generation for System Log
FAU_SAA.1/SYS	Potential violation analysis for System Log
FAU_SAR.1/SYS	Audit review for System Log
FAU_STG.4/SYS	Prevention of audit data loss for the System Log
FAU_GEN.1/CON	Audit data generation for Consumer Log
FAU_SAR.1/CON	Audit review for Consumer Log
FAU_STG.4/CON	Prevention of audit data loss for the Consumer Log
FAU_GEN.1/CAL	Audit data generation for Calibration Log
FAU_SAR.1/CAL	Audit review for Calibration Log
FAU_STG.4/CAL	Prevention of audit data loss for the Calibration Log
FAU_GEN.2	User identity association

FAU_STG.2	Guarantees of audit data availability
Class FCO: Communication	
FCO_NRO.2	Enforced proof of origin
Class FCS: Cryptographic Support	
FCS_CKM.1/TLS	Cryptographic key generation for TLS
FCS_COP.1/TLS	Cryptographic operation for TLS
FCS_CKM.1/CMS	Cryptographic key generation for CMS
FCS_COP.1/CMS	Cryptographic operation for CMS
FCS_CKM.1/MTR	Cryptographic key generation for Meter communication encryption
FCS_COP.1/MTR	Cryptographic operation for Meter communication encryption
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1/HASH	Cryptographic operation for Signatures
FCS_COP.1/MEM	Cryptographic operation for TSF and user data encryption
Class FDP: User Data Protection	
FDP_ACC.2	Complete Access Control
FDP_ACF.1	Security attribute based access control
FDP_IFC.2/FW	Complete information flow control for firewall
FDP_IFF.1/FW	Simple security attributes for Firewall
FDP_IFC.2/MTR	Complete information flow control for Meter information flow
FDP_IFF.1/MTR	Simple security attributes for Meter information
FDP_RIP.2	Full residual information protection
FDP_SDI.2	Stored data integrity monitoring and action
Class FIA: Identification and Authentication	
FIA_ATD.1	User attribute definition
FIA_AFL.1	Authentication failure handling
FIA_UAU.2	User authentication before any action
FIA_UAU.5	Multiple authentication mechanisms
FIA_UAU.6	Re-Authenticating

FIA_UID.2	User identification before any action
FIA_USB.1	User-subject binding
Class FMT: Security Management	
FMT_MOF.1	Management of security functions behaviour
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FMT_MSA.1/AC	Management of security attributes for Gateway access policy
FMT_MSA.3/AC	Static attribute initialisation for Gateway access policy
FMT_MSA.1/FW	Management of security attributes for firewall policy
FMT_MSA.3/FW	Static attribute initialisation for Firewall policy
FMT_MSA.1/MTR	Management of security attributes for Meter policy
FMT_MSA.3/MTR	Static attribute initialisation for Meter policy
Class FPR: Privacy	
FPR_CON.1	Communication Concealing
FPR_PSE.1	Pseudonymity
Class FPT: Protection of the TSF	
FPT_FLS.1	Failure with preservation of secure state
FPT_RPL.1	Replay Detection
FPT_STM.1	Reliable time stamps
FPT_TST.1	TSF testing
FPT_PHP.1	Passive detection of physical attack
Class FTP: Trusted path/channels	
FTP_ITC.1/WAN	Inter-TSF trusted channel for WAN
FTP_ITC.1/MTR	Inter-TSF trusted channel for Meter
FTP_ITC.1/USR	Inter-TSF trusted channel for User

Table 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 • Billing-relevant data needed to verify an invoice • 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	• 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 [create a log entry within the System Log]*] 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 **as listed in Table 12**; and c) [*other non-privacy relevant auditable events as listed in Table 13*].
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, [*all information as listed in Table 14 conforming to [FNN Log]*].
Hierarchical to:	No other components
Dependencies:	FPT_STM.1

SFR	Auditable Events	Refinement justification
FAU_ARP.1/SYS	Actions taken due to potential security violations.	
FAU_GEN.1/SYS	-	
FAU_GEN.1/CON	-	
FAU_GEN.1/CAL	-	
FAU_GEN.2	-	
FAU_SAA.1/SYS	Enabling and disabling of any of the analysis mechanisms. Automated responses performed by the tool.	
FAU_SAR.1/SYS	Reading of information from the audit records.	
FAU_SAR.1/CON	Reading of information from the audit records.	
FAU_SAR.1/CAL	Reading of information from the audit records.	
FAU_STG.2	-	
FAU_STG.4/SYS	Actions taken due to the audit storage failure.	
FAU_STG.4/CON	Actions taken due to the audit storage failure.	
FAU_STG.4/CAL	Actions taken due to the audit storage failure.	

SFR	Auditable Events	Refinement justification
FCO_NRO.2	The invocation of the non-repudiation service. Identification of the information, the destination, and a copy of the evidence provided	
FCS_CKM.1/CMS	Success and failure of the activity. The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).	
FCS_CKM.1/MTR	Success and failure of the activity. The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).	
FCS_CKM.1/TLS	Success and failure of the activity. The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).	
FCS_CKM.4	Success and failure of the activity. The object attribute(s), and object value(s) excluding any sensitive information (e.g. secret or private keys).	
FCS_COP.1/CMS	Success and failure, and the type of cryptographic operation. Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.	
FCS_COP.1/HASH	Success and failure, and the type of cryptographic operation. Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.	
FCS_COP.1/MEM	~~**Success and failure, and the type of cryptographic operation.**~~ ~~**Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.**~~	The setup is done during boot without access to the System Log. Afterwards, the encryption and decryption is done transparently without a possibility to fail. The type of cryptographic operation is fixed within this ST.

SFR	Auditable Events	Refinement justification
FCS_COP.1/MTR	Success and failure, and the type of cryptographic operation. Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.	
FCS_COP.1/TLS	Success and failure, and the type of cryptographic operation. Any applicable cryptographic mode(s) of operation, subject attributes and object attributes.	
FDP_ACC.2	-	
FDP_ACF.1	All requests to perform an operation on an object covered by the SFP.	
FDP_IFC.2/FW	-	
FDP_IFC.2/MTR	-	
FDP_IFF.1/FW	All decisions on requests for information flow.	
FDP_IFF.1/MTR	All decisions on requests for information flow.	
FDP_RIP.2	-	
FDP_SDI.2	All attempts to check the integrity of user data, including an indication of the results of the check, if performed.	
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions taken and the subsequent, if appropriate, restoration to the normal state.	
FIA_ATD.1	-	
FIA_UAU.2	All use of the authentication mechanism.	
FIA_UAU.5	The result of each activated mechanism together with the final decision.	
FIA_UAU.6	All reauthentication attempts.	
FIA_UID.2	All use of the user identification mechanism, including the user identity provided.	
FIA_USB.1	Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).	

SFR	Auditable Events	Refinement justification
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF.	
FMT_MSA.1/AC	All modifications of the values of security attributes.	
FMT_MSA.1/FW	All modifications of the values of security attributes.	
FMT_MSA.1/MTR	All modifications of the values of security attributes.	
FMT_MSA.3/AC	~~**All modifications of the initial values of security attributes.**~~	Initial values can not be changed
FMT_MSA.3/FW	~~**All modifications of the initial values of security attributes.**~~	Initial values can not be changed
FMT_MSA.3/MTR	~~**All modifications of the initial values of security attributes.**~~	Initial values can not be changed
FMT_SMF.1	Use of the management functions.	
FMT_SMR.1	Modifications to the group of users that are part of a role.	
FPR_CON.1	-	
FPR_PSE.1	~~**The subject/user that requested resolution of the user identity should be audited.**~~	The TOE does not allow resolution of the pseudonym to the user identity.
FPT_FLS.1	Failure of the TSF.	
FPT_PHP.1	~~**If detection by IT means, detection of intrusion.**~~	Outside the scope of the TOE
FPT_RPL.1	Detected replay attacks.	
FPT_STM.1	Changes to the time	
FPT_TST.1	Execution of the TSF self tests and the results of the tests.	
FTP_ITC.1/MTR	All attempted uses of the trusted channel functions. Identification of the initiator and target of all trusted channel functions.	
FTP_ITC.1/USR	All attempted uses of the trusted channel functions. Identification of the initiator and target of all trusted channel functions.	

SFR	Auditable Events	Refinement justification
FTP_ITC.1/WAN	All attempted uses of the trusted channel functions. Identification of the initiator and target of all trusted channel functions.	

Table 12: Auditable Events for System Log

Gateway specific auditable events
Updates of the identification used by the TOE to authenticate against users.
Updates in the firmware update process.
Start of the TOE firmware.

Table 13: Other auditable Events for System Log

Entry	Description
record_number	Unique entry identifier in each logbook.
parent_record_number	unused
repetition_counter	Shows the first and last appearance of one successive repetitive logmessage
seconds_index	Unix timestamp of when the event occurred
timestamp	ISO8601 Date and Time of when the event occurred
level	Severity level of the log entry: • Info, general information • Warning, unexpected event • Error, rectifiable error • Fatal, fatal error, process was stopped • Extension, system specific error

Entry	Description
type	The event identifier, contains: • version: Version of the logsystem • length: *unused* • device_type: specifies the logmessage origin device (unknown, SMGw, CLS, GWA, EMT) • module: defines a module within the device as the event source • function: *unused* • vendor_id: specifies the vendor for this logmessage • event_id: specifies one event • event_sub_id: gives more detailed information
outcome	Outcome of the performed action: • Success, action succeeded • Failure, action failed • Extension, system specific outcome
subject_identity	Identity of the subject that causes the event (or empty, if the identity of the subject is unknown).
user_identity	Identification of the user, if provided, contains: • logical_name • class_id • class_version
message_extensions	Contains message parts which can be used to produce language independent logmessages with a log interpreter (if applicable)
peer_identity	Identity of the communication partner (if applicable).
evidence	Signature (if applicable).

Table 14: Information that shall be logged conforming to [FNN Log]

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 [• *a defined number of authentication failures from a specific device or IP address* • *a defined number of reboots per day* • *a defined number of system logmessages per hour* • *a process restarted* • *a defined number of concurrent connections or connection attempts to a service from a specific IP address in the HAN*] known to indicate a potential security violation; b) [*None*].
Hierarchical to:	No other components
Dependencies:	FAU_GEN.1
Application Note 4:	All types of failures in the TSF as listed in FPT_FLS.1 will directly be recognized as a potential violation by the TOE. It is not relied upon monitoring the audited events in order to detect them.

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 the Gateway Administrator*] if the **system** 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 5:	The size of the audit trail that is available before the oldest events get overwritten is configurable for the Gateway Administrator.

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 15 and [none]*].
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 15 and [none]*].
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	-

Table 15: Events for the 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
Dependencies:	FAU_GEN.1
Application Note 6:	FAU_SAR.1.2/CON shall ensure that the consumer is able to interpret the information that is provided to him in a way that allows him to verify the invoice.

6.2.3.3 Security audit event storage (FAU_STG)

6.2.3.3.1 FAU_STG.4/CON: Prevention of audit data loss for the Consumer Log

FAU_STG.4.1/CON	The TSF shall [overwrite the oldest stored audit records] and [*inform the Gateway Administrator*] if the **consumer** audit trail is full.
Hierarchical to:	FAU_STG.3 Action in case of possible audit data loss
Dependencies:	FAU_STG.1 Protected audit trail storage
Application Note 7:	The size of the audit trail that is available before the oldest events get overwritten is configurable for the Gateway Administrator.

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 audit events required by [PTB A50.8, Table 4-23] as listed in Table 16*].
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, [*additional information as listed in Table 16 and Table 14*].
Hierarchical to:	No other components
Dependencies:	FPT_STM.1
Application Note 8:	The Calibration Log serves to fulfil national requirements in the context of the calibration of the TOE.

Event	Additional Information
Start of operation of the SMGW	Start of operation as well as the responsible calibration authority
Start of a self test	-
Adding and removal of a Meter	-
Adding and removal of a processing profile	-

Event	Additional Information
A change of a processing profile	Parameters of a processing profile for which a change leads to an entry: • Device IDs of the Meters used for this processing profile • OBIS code of the measured values of any Meter • Measuring point id • Billing period • Consumer id • Validity period • Definition of tariffs • Tariff switching times • Registering period
Adding and removal of a meter profile	-
A change of a meter profile	Parameters of a meter profile for which a change leads to an entry: • Device ID of the Meter • Key material used for inner signature • Registering period • Display intervall of Meter data • Indication whether the meter sums up positive and negative energy flow • OBIS codes of the measured values • Transformer factors
Software update	Update of the calibration relevant part of the software
Firmware update	Every firmware update
A fatal error reported by the Meter	Meter-ID of the reporting Meter
A calibration-relevant error detected by the Gateway	Errors, such as • Power Outage exceeds power reserve of the RTC • Deviation between the local time and the reliable timesource provided by the Gateway Administrator is too large • Events which may lead to a corruption of meter data

Table 16: Events for the Calibration Log as required by [PTB A50.8]

6.2.4.2 Security audit review (FAU_SAR)

6.2.4.2.1 FAU_SAR.1/CAL: Audit Review for 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 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 9:	As outlined in the introduction it has to be ensured that the events of the Calibration Log are available over the lifetime of the TOE.

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 10:	Please note that FAU_GEN.2 applies to all audit logs, the System Log, the Calibration Log, and the Consumer Log.

6.2.5.2 Security audit event storage (FAU_STG)

6.2.5.2.1 FAU_STG.2: Guarantees of audit data availability

FAU_STG.2.1	The TSF shall protect the stored audit records in ~~**the**~~ **all** audit trail**s** 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 [*all of the Calibration Log audit records and at least the last 15 months of the other logs*] 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
Application Note 11:	Please note that FAU_STG.2 applies to all audit logs, the System Log, the Calibration Log, and the Consumer Log.

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*[36]] 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 [TR 03109-1]*].
Hierarchical to:	FCO_NRO.1 Selective proof of origin
Dependencies:	FIA_UID.1 Timing of identification
Application Note 12:	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.
Application Note 13:	Meter Data that is pseudonymised according to FPR_PSE.1 must not carry any evidence of origin, as such a signature would allow resolution of the pseudonym to the Gateway identity (see also [TR 03109-1 Errata TAF9/10]). Therefore the TOE removes any signatures generated according to FCO_NRO.2 prior to transmission of pseudonymised Meter Data to external entities.

[36] 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_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* *combined with a specified cryptographic elliptic curve* • *secp256r1 (prime256v1, NIST P-256)* • *secp384r1 (ansip384r1, NIST P-384)* • *brainpoolP256r1* • *brainpoolP384r1* • *brainpoolP512r1*] and specified cryptographic key sizes [*128 bit, 256 bit*] that meet the following: [• *TLS_ECDHE_ECDSA_WITH_AES_xxx_xxx_SHAxxx: [RFC 5289]* • *ECDHE: [TR 03111]* • *TLS PRF: [RFC 5246]* • *HMAC: [RFC 2104]* • *SHAxxx: [FIPS 180-4]* • *secpxxxr1: [SECG-SEC2]* • *brainpoolPxxxr1: [RFC 5639]*].
Hierarchical to:	No other components
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation], fulfilled by FCS_COP.1/TLS FCS_CKM.4 Cryptographic key destruction
Application Note 14:	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* *combined with a specified cryptographic elliptic curve* • *secp256r1 (prime256v1, NIST P-256)* • *secp384r1 (ansip384r1, NIST P-384)* • *brainpoolP256r1* • *brainpoolP384r1* • *brainpoolP512r1*] and cryptographic key sizes [*128 bit, 256 bit*] that meet the following: [• *TLS_ECDHE_ECDSA_WITH_AES_xxx_xxx_SHAxxx: [RFC 5289]* • *ECDSA: [TR 03111]* • *AES: [FIPS 197]* • *GCM: [NIST SP800-38D]* • *CBC: [NIST SP800-38A]* • *HMAC: [RFC 2104]* • *SHAxxx: [FIPS 180-4]* • *secpxxxr1: [SECG-SEC2]* • *brainpoolPxxxr1: [RFC 5639]*].
Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], fulfilled by FCS_CKM.1/TLS FCS_CKM.4 Cryptographic key destruction

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-X963KDF-SHA256* • *ecka-eg-X963KDF-SHA384* • *ecka-eg-X963KDF-SHA512* *combined with a specified key encryption algorithm* • *id-aes128-wrap* • *id-aes192-wrap* • *id-aes256-wrap*] and specified cryptographic key sizes [*128bit, 192bit, 256bit*] that meet the following: [*ecka-eg-X963KDF-SHAxxx: [TR 03111], id-aesxxx-wrap: [RFC 3394]*].
Hierarchical to:	No other components

Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation], fulfilled by FCS_COP.1/CMS FCS_CKM.4 Cryptographic key destruction
Application Note 15:	The TOE utilises the services of its Security Module for 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-aes128-GCM* • *id-aes192-GCM* • *id-aes256-GCM* • *id-aes-CBC-CMAC-128* • *id-aes-CBC-CMAC-192* • *id-aes-CBC-CMAC-256*] and cryptographic key sizes [*128bit, 192bit, 256bit*] that meet the following: [• *AES: [FIPS 197]* • *GCM: [NIST SP800-38D]* • *CBC: [NIST SP800-38A]* • *CMAC: [NIST SP800-38B]* • *id-aesxxx-CBC: [RFC 3565]* • *id-aesxxx-gcm: [RFC 5084]* • *id-aes-CBC-CMAC-xxx: [TR 03109-1-I]*].
Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], fulfilled by FCS_CKM.1/CMS FCS_CKM.4 Cryptographic key destruction

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*] and specified cryptographic key sizes [*128bit*] that meet the following: [• *AES-CMAC: [RFC 4493]* • *AES: [FIPS 197]* • *CMAC: [NIST SP800-38B]*].

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, integrity protection*] in accordance with a specified cryptographic algorithm [*AES_CBC and AES-CMAC*] and cryptographic key sizes [*128bit*] that meet the following: [• *AES: [FIPS 197]* • *CBC: [NIST SP800-38A]* • *AES-CMAC: [RFC 4493]* • *CMAC: [NIST SP800-38B]*].
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 16: 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
    1) the key is being generated by the Gateway periodically according to [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
    2) 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.

Application Note 17: If the connection between the Meter and TOE is unidirectional, the communication between the Meter and the TOE is secured by the use of a symmetric AES encryption. If a bidirectional connection between the Meter and the TOE is established, the communication is secured by a TLS channel as described in chapter 6.4.1. As the TOE shall be interoperable with all kind of Meters it implements both kinds of encryption.

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*] that meets the following: [*[FIPS 140-2], [RFC 4493]*].
Hierarchical to:	No other components
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation], fulfilled by FCS_CKM.1/TLS and FCS_CKM.1/CMS and FCS_CKM.1/MTR.
Application Note 18:	Please note that as against the requirement FDP_RIP.2 the mechanisms implementing the requirement from FCS_CKM.4 shall be suitable to avoid attackers with physical access to the TOE from accessing the keys after they are no longer used.

6.4.4.2 Cryptographic operation (FCS_COP)

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

FCS_COP.1.1/HASH	The TSF shall perform [*hashing for signature creation and verification*] in accordance with a specified cryptographic algorithm [*SHA-256, SHA-384, SHA-512*] and cryptographic key sizes [*none*] that meet the following: [*[FIPS 180-4]*].
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[37]] FCS_CKM.4 Cryptographic key destruction
Application Note 19:	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 [*XTS-AES*] and cryptographic key sizes [*128bit*] that meet the following: [*[FIPS 197], [IEEE P1619]*].
Hierarchical to:	No other components

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

Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] ~~, fulfilled by FCS_CKM.1/CMS~~[38] FCS_CKM.4 Cryptographic key destruction
Application Note 20:	Please note that the key generation functionality of the Security Module is used for TSF and user data encryption, not the key generation functionality as defined by FCS_CKM.1/CMS.
Application Note 21:	The TOE encrypts its local TSF and user data while it is not in use (i.e. while stored in a persistent memory). The Security Module is used to store the symmetric key that is used for the encryption of TSF and user data. It shall be noted that this kind of encryption cannot provide an absolute protection against physical manipulation and does not aim to. It however contributes to the security concept that considers the protection that is provided by the environment.

6.5 Class FDP: User Data Protection

6.5.1 Introduction to the Security Functional Policies

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

- The Gateway access SFP is an access control policy to control the access to objects under the control of the TOE. The details of this access control policy highly depend on the concrete application of the TOE. The access control policy is described in more detail in [TR 03109-1].
- The Firewall SFP implements an information flow policy to fulfil the objective O.Firewall. All requirements around the communication control that the TOE poses on communications between the different networks are defined in this policy.
- The Meter SFP implements an information flow policy to fulfil the objective O.Meter. It defines all requirements concerning how the TOE shall handle Meter Data.

6.5.2 Gateway Access SFP

6.5.2.1 Access control policy (FDP_ACC)

6.5.2.1.1 FDP_ACC.2: Complete access control

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

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

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,* [• *only authorised Gateway Administrators are allowed to read the Calibration Log*, • *only authorised Gateway Administrators are allowed to manage the Gateway config*, • *the TOE only downloads FW updates from authorised Gateway Administrators*, • *the TOE only synchronizes its Gateway time with a reliable time source of authorised Gateway Administrators*, • *Meter Data shall be transmitted only via the interface IF_GW_MTR to the Gateway, only via IF_GW_WAN to the authorised EMT and only via IF_GW_CON to the authorised Consumer*.]].
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].
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*].
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 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/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: 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=HAN or source_interface=LMN) and* *destination_interface=TOE and* *source_authenticated=true* *Connection establishment is allowed* *if source_interface=TOE and* *(destination_interface=LMN or destination_interface=HAN) and* *destination_authenticated = true* *Connection establishment is allowed* *]* *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*].
Hierarchical to:	No other components
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
Application Note 22:	It should be noted that the FDP_IFF.1.1/FW facilitates different interfaces of the origin and the destination of an information flow implicitly requires the TOE to implement physically separate ports for WAN, LMN and HAN.

6.5.4 Meter SFP

6.5.4.1 Information flow control policy (FDP_IFC)

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

FDP_IFC.2.1/MTR	The TSF shall enforce the [*Meter SFP*] 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

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 Profile*].
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] within a synchronization interval between 90 seconds and 3 hours].* ▪ *If the deviation between the local time and the remote time is acceptable*[39] *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*[40] *and* • *inform a Gateway Administrator*].
FDP_IFF.1.4/MTR	The TSF shall explicitly authorise an information flow based on the following rules: [*none*].
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 FMT_MSA.3 Static attribute initialisation

[39] Please refer to the following application note for a detailed definition of "acceptable"

[40] 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.

Application Note 23: FDP_IFF.1.3 defines that the TOE shall update the local system time regularly with a reliable external time sources if the deviation is acceptable. In the context of this functionality two aspects should be mentioned:

Reliability of external source

To achieve the reliablity of the external source the TOE only synchronises the local time with a time source provided by the Gateway Administrator.

Acceptable deviation

For the question whether a deviation between the time source(s) in the WAN and the local system time is still acceptable, normative or legislative regulations are considered. Therefore, a maximum deviation of 3% of the measuring period is allowed to be in conformance with this Security Target.

Application Note 24: In FDP_IFF.1.5/MTR the TOE is required to verify the authenticity, integrity and confidentiality of the Meter Data received from the Meter. The TOE has two options to do so:

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

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

6.5.5 General Requirements on user data protection

6.5.5.1 Residual information protection (FDP_RIP)

6.5.5.1.1 FDP_RIP.2: Full residual information protection

FDP_RIP.2.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [deallocation of the resource from] all objects.
Hierarchical to:	FDP_RIP.1 Subset residual information protection
Dependencies:	No dependencies.

Application Note 25: 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 not 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*] on all objects, based on the following attributes: [• *database integrity check for Meter Data.* – *out-of-order records* – *missing pages* – *malformed records* – *constraint errors* • *hash value check for System, Consumer and Calibration log data.*]
FDP_SDI.2.2	Upon detection of a data integrity error, the TSF shall [*create a System Log entry, go into lock-down mode*[41] *and inform the Gateway Administrator*].
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring
Dependencies:	No dependencies.
Application Note 26:	This Security Target defines that the TOE shall be capable of detecting integrity errors on all objects.

6.6 Class FIA: Identification and Authentication

6.6.1 User Attribute Definition (FIA_ATD)

6.6.1.1 FIA_ATD.1: User attribute definition

FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [• *User Identity* • *Status of Identity (Authenticated or not)* • *Connecting network (WAN, HAN or LMN)* • *Role membership* • *[None]*].
Hierarchical to:	No other components.
Dependencies:	No dependencies.

6.6.2 Authentication Failures (FIA_AFL)

6.6.2.1 FIA_AFL.1: Authentication Failure handling

FIA_AFL.1.1	The TSF shall detect when [**a Gateway** Administrator configurable positive integer within [*3 and 10*]] 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 [*inform the Gateway Administrator, create a Consumer Log entry (if the user ID is known), create a System Log entry and lock the user account for 5 minutes*].

[41] Please refer to section 7.7 for more details on the lock-down mode.

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

6.6.3.2 FIA_UAU.5: Multiple authentication mechanisms

FIA_UAU.5.1	The TSF shall provide [• *authentication via certificates at the IF_GW_MTR interface,* • *TLS-authentication via certificates at the IF_GW_WAN interface,* • *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 **via HAN-certificates** 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 28:	Please refer to [TR 03109-1] for a more detailed overview on the authentication of the TOE users.

6.6.3.3 FIA_UAU.6: Re-authenticating

FIA_UAU.6.1	The TSF shall re-authenticate ~~**the user**~~ **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 29:	This requirement on re-authentication for external entities in the WAN and LMN is addressed by disconnecting the TLS channel even though a re-authentication is – strictly speaking – only achieved if the TLS channel is build up again.
Application Note 30:	The term "other local users" refers to "authorised Consumer" and "authorised Service Technician".

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: [

- *the user identity is set to the identity of the login credentials,*
- *the connecting network is set to the interface on which the authentication was done,*
- *the status of identity is set to authenticated if the user provided the correct login credentials and used the correct connecting network as defined by the corresponding Gateway config, otherwise it is set to not authenticated,*
- *the role is set to the value as defined by the corresponding processing profile*

].

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 of an active user is not alterable,*
- *the connecting network of an active user is not alterable,*
- *the role of an active user is not alterable,*
- *the status of identity of an active user is set to not authenticated if a condition of FIA_UAU.6 is fulfilled or the corresponding Gateway config gets deleted by the Gateway Administrator*

].

Hierarchical to: No other components.

Dependencies: FIA_ATD.1 User attribute definition

6.7 Class FMT: Security Management

6.7.1 Management of the TSF

6.7.1.1 Management of functions in TSF

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*].

Hierarchical to: No other components.

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

Function	Limitation
Display the version number of the TOE Display the current time	The management functions must only be accessible for an authorised consumer ~~**and only**~~ via the interface IF_GW_CON **, for an authorised Gateway Administrator via the interface IF_GW_WAN and for an authorised Service Technician via the interface IF_GW_SRV**.
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[42]
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, Table 20 and [none]*].
Hierarchical to:	No other components.
Dependencies:	No dependencies.

SFR	Management functionality	Refinement justification
FAU_ARP.1/SYS	• ~~**The management (addition, removal, or modification) of actions.**~~	Actions are fixed within this ST
FAU_GEN.1/SYS FAU_GEN.1/CON FAU_GEN.1/CAL	-	
FAU_SAA.1/SYS	• Maintenance of the rules by (adding, modifying, deletion) of rules from the set of rules.	

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

SFR	Management functionality	Refinement justification
FAU_SAR.1/SYS FAU_SAR.1/CON FAU_SAR.1/CAL	-[43]	
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.	Actions are fixed within this ST
FAU_STG.4/CAL	- [44]	
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 of evidence.	
FCS_CKM.1/TLS	-	
FCS_COP.1/TLS	• Management of key material including key material stored in the Security Module	
FCS_CKM.1/CMS	-	
FCS_COP.1/CMS	• Management of key material including key material stored in the Security Module	
FCS_CKM.1/MTR	-	
FCS_COP.1/MTR	• Management of key material stored in the Security Module and key material brought into the gateway during the pairing process.	
FCS_CKM.4	-	
FCS_COP.1/HASH	-	
FCS_COP.1/MEM	• ~~**Management of key material**~~	The key material is not alterable.
FDP_ACC.2	-	

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

[44] 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 justification
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~~.	
FDP_IFC.2/MTR	-	
FDP_IFF.1/MTR	• Managing the attributes (including Processing Profiles) used to make explicit access based decisions.	
FDP_RIP.2	-	
FDP_SDI.2	• ~~**The actions to be taken upon the detection of an integrity error shall be configurable.**~~	Actions are fixed within this ST
FIA_ATD.1	• If so indicated in the assignment, the authorised Gateway Administrator might be able to define additional security attributes for users.	
FIA_AFL.1	• Management of the threshold for unsuccessful authentication attempts; • ~~**Management of actions to be taken in the event of an authentication failure.**~~	Actions are fixed within this ST.
FIA_UAU.2	• Management of the authentication data by an Gateway Administrator;	
FIA_UAU.5	- [45]	
FIA_UAU.6	- [45]	
FIA_UID.2	• The management of the user identities.	

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

SFR	Management functionality	Refinement justification
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.	
FMT_MOF.1	• Managing the group of roles that can interact with the functions in the TSF.	
FMT_SMF.1	-	
FMT_SMR.1	• Managing the group of users that are part of a role.	
FMT_MSA.1/AC	• ~~**Management of rules by which security attributes inherit specified values.**~~[46]	Rules are fixed within the TOE.
FMT_MSA.3/AC	- [47]	
FMT_MSA.1/FW	• ~~**Management of rules by which security attributes inherit specified values.**~~[48]	Rules are fixed within the TOE.
FMT_MSA.3/FW	- [47]	
FMT_MSA.1/MTR	• ~~**Management of rules by which security attributes inherit specified values.**~~[48]	Rules are fixed within the TOE.
FMT_MSA.3/MTR	- [47]	
FPR_CON.1	• Definition of the interval in FAU_CON.1.2 if definable within the operational phase of the TOE	
FPR_PSE.1	-	
FPT_FLS.1	-	
FPT_RPL.1	-	
FPT_STM.1	• Management of a time source.	
FPT_TST.1	- [49]	

[46] As the role that can interact with the security attributes is restricted to the Gateway Administrator within this ST not all management functions as defined by Common Criteria part 2 do apply.

[47] 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.

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

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

SFR	Management functionality	Refinement justification
FPT_PHP.1	• ~~**Management of the user or role that determines whether physical tampering has occurred.**~~	Outside the scope of the TOE.
FTP_ITC.1/WAN	- [50]	
FTP_ITC.1/MTR	- [50]	
FTP_ITC.1/USR	- [50]	

Table 19: SFR related Management Functionalities

Gateway specific Management Functionalities
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[51]

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,* *[none]*].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Hierarchical to:	No other components.
Dependencies:	No dependencies.

apply.

[50] 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.

[51] 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.

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*]] 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*]] 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.

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

6.7.5 Management of security attributes for Meter SFP

6.7.5.1 Management of security attributes (FMT_MSA)

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

FMT_MSA.1.1/MTR	The TSF shall enforce the [*Meter SFP*] to restrict the ability to [change_default, query, modify, delete, [*none*]] 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

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 [*the load or size of Meter Data or the frequency (including the absence) of sending it to authorized External Entities*].
FPR_CON.1.2	The TSF shall connect to [*authorized External Entities as defined within the Processing Profiles*] in intervals as follows [*a Gateway Administrator configurable interval between a minute and a year*] 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 [*following alias metric:* • *the alias must not contain the Meter Identity,* • *the alias must not contain the Gateway Identity,* • *the alias must not contain the Consumer Identity,*].
Hierarchical to:	No other components.
Dependencies:	No dependencies.

Application Note 32: 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 those cases the TOE shall replace the identity of the consumer by a pseudonymous identifier. Please note that the identity of the consumer may not be their name but could also be a number (e.g. consumer ID) used for billing purposes.

A Gateway may use more than one pseudonymous identifier.

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

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

6.9 Class FPT: Protection of the TSF

6.9.1 Fail secure (FPT_FLS)

6.9.1.1 FPT_FLS.1: Failure with preservation of secure state

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

- *the deviation between the local system time of the TOE and the reliable external time source is too large,*
- *[*
  - *the self test fails,*
  - *the calibration log is full,*
  - *the communication with the security module fails,*
  - *the power supply breaks down*

  ]

].

Hierarchical to: No other components.

Dependencies: No dependencies.

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 33:	The time stamps as defined by FPT_STM.1 shall be of sufficient exactness. Therefore, the local system time of the TOE is synchronised regularly with a reliable external time source provided by the Gateway Administrator. Radio controlled clocks are not used. However, the local clock has a sufficient exactness as the synchronisation will fail if the deviation is too large (the TOE will preserve a secure state according to FPT_FLS.1). A maximum deviation of 3% of the measuring period is allowed. Further the TOE provides a Real Time Clock (RTC) that is used to set the internal system time of the TOE after a power cut.

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.

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.
Application Note 34:	The level of protection that is required by FPT_PHP.1 is the same level of protection that is expected for classical meters. The passive detection of a physical attack is achieved by a seal that is affixed at the Gateway in a way that it is not possible to open the casing of the Gateway without visible tampering of the seal.

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**] 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.
Application Note 35:	The corresponding cryptographic primitives are defined by FCS_COP.1/MTR.

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

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

6.11 Security Assurance Requirements for the TOE

The minimum Evaluation Assurance Level for this Security Target is **EAL 4 augmented by AVA_VAN.5 and ALC_FLR.2.**
The following table lists the assurance components which are therefore applicable to this ST.

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

Assurance Class	Assurance Component
	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								

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Management	O.Log	O.Access
FDP_IFF.1/FW	X	X								
FDP_IFC.2/MTR				X		X				
FDP_IFF.1/MTR				X		X				
FDP_RIP.2							X			
FDP_SDI.2							X			
FIA_ATD.1								X		
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	

	O.Firewall	O.SeparateIF	O.Conceal	O.Meter	O.Crypt	O.Time	O.Protect	O.Management	O.Log	O.Access
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 LAN have been interchanged.

6.12.1.1.3 O.Conceal

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

6.12.1.1.4 O.Meter

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

- **FDP_IFC.2/MTR** and **FDP_IFF.1/MTR** define an information flow policy to introduce how the Gateway shall handle Meter Data.
- **FCO_NRO.2** 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 pseudonymization of Meter identities for Status data.
- **FTP_ITC.1/MTR** defines the requirements around the Trusted Channel that shall be implemented by the Gateway in order to protect information submitted via the Gateway and external entities in the WAN or the Gateway and a distributed Meter.

6.12.1.1.5 O.Crypt

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

- **FCS_CKM.4** defines the requirements around the secure deletion of ephemeral cryptographic keys.
- **FCS_CKM.1/TLS** defines the requirements on key negotiation for the TLS protocol.
- **FCS_CKM.1/CMS** defines the requirements on key generation for symmetric encryption within CMS.
- **FCS_COP.1/TLS** defines the requirements around the encryption and decryption capabilities of the Gateway for communications with external entities 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 Administrators via the IF_GW_WAN interface.

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

6.12.1.1.10 O.Access

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

6.12.1.2 Fulfilment of the dependencies

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

SFR	Dependencies	Fulfilled by
FAU_ARP.1/SYS	FAU_SAA.1 Potential violation analysis	FAU_SAA.1/SYS
FAU_GEN.1/SYS	FPT_STM.1 Reliable time stamps	FPT_STM.1
FAU_SAA.1/SYS	FAU_GEN.1 Audit data generation	FAU_GEN.1/SYS
FAU_SAR.1/SYS	FAU_GEN.1 Audit data generation	FAU_GEN.1/SYS
FAU_STG.4/SYS	FAU_STG.1 Protected audit trail storage	FAU_STG.2
FAU_GEN.1/CON	FPT_STM.1 Reliable time stamps	FPT_STM.1
FAU_SAR.1/CON	FAU_GEN.1 Audit data generation	FAU_GEN.1/CON
FAU_STG.4/CON	FAU_STG.1 Protected audit trail storage	FAU_STG.2
FAU_GEN.1/CAL	FPT_STM.1 Reliable time stamps	FPT_STM.1
FAU_SAR.1/CAL	FAU_GEN.1 Audit data generation	FAU_GEN.1/CAL
FAU_STG.4/CAL	FAU_STG.1 Protected audit trail storage	FAU_STG.2
FAU_GEN.2	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification	FAU_GEN.1/SYS FAU_GEN.1/CON FIA_UID.2
FAU_STG.2	FAU_GEN.1 Audit data generation	FAU_GEN.1/SYS FAU_GEN.1/CON FAU_GEN.1/CAL
FCO_NRO.2	FIA_UID.1 Timing of identification	FIA_UID.2
FCS_CKM.1/TLS	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/TLS FCS_CKM.4
FCS_COP.1/TLS	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1/TLS FCS_CKM.4
FCS_CKM.1/CMS	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1/CMS FCS_CKM.4

SFR	Dependencies	Fulfilled by
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

SFR	Dependencies	Fulfilled by
FDP_IFF.1/MTR	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	FDP_IFC.2/MTR FMT_MSA.3/MTR
FDP_RIP.2	-	-
FDP_SDI.2	-	-
FIA_ATD.1	-	-
FIA_AFL.1	FIA_UAU.1 Timing of authentication	FIA_UAU.2
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UAU.5	-	-
FIA_UAU.6	-	-
FIA_UID.2	-	-
FIA_USB.1	FIA_ATD.1 User attribute definition	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_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

SFR	Dependencies	Fulfilled by
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 TSF and user data encryption as defined by FCS_COP.1/MEM uses the functionality of the Security Module for key generation. As such the dependency to an import or generation of key material is omitted for this SFR.

6.12.2 Security Assurance Requirements rationale

The decision on the assurance level has been mainly driven by the assumed attack potential. As outlined in the previous chapters of this Security Target it is assumed that – at least from the WAN side – a high attack potential is posed against the security functions of the TOE. This leads to the use of AVA_VAN.5 (Resistance against high attack potential).
In order to keep evaluations according to this Security Target commercially feasible EAL 4 has been chosen as assurance level as this is the lowest level that provides the prerequisites for the use of AVA_VAN.5.
Eventually, the augmentation by ALC_FLR.2 has been chosen to emphasize the importance of a structured process for flaw remediation at the developers 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

7.1 SF.AU: Audit

The TOE maintains three kinds of logs:

- System Log
- Consumer Log
- Calibration Log

The purpose of the **System Log** is to inform the Gateway Administrator and the Service Technician about the system status of the Smart Meter Gateway. Therefore the TOE records within this log all system relevant events as listed in Table 12 and Table 13 (**FAU_GEN.1.1/SYS**). No privacy relevant information (e.g. Meter Data) are stored within the system log. Only the authorized Gateway Administrator using IF_GW_WAN and authorized Service Technicians via IF_GW_SRV are able to read this log file (**FAU_SAR.1/SYS**).
To indicate any potential security violations the TOE monitors the audited events (**FAU_SAA.1/SYS**). Thereby the TOE applies the following set of rules: The TOE detects a potential security violation, if at least one of the following events occur:

- a defined number of authentication failures from a specific device or IP address
- a defined number of reboots per day
- a defined number of system logmessages per hour
- a process restarted
- a defined number of concurrent connections or connection attempts to a service from a specific IP address in the HAN

Upon detection of a potential security violation the TOE generates a log entry within the system log and informs the Gateway Administrator via the communication scenario “ADMIN-SERVICE” as described in [TR 03109-1], chapter 3.2.3.2 (**FAU_ARP.1/SYS**).
If the system audit trail is full, the TOE deletes a defined number of the oldest events. Whenever the TOE deletes old log events, it informs the Gateway Administrator and creates a log entry that the audit trail was cleaned up within the system log (**FAU_STG.4/SYS**). It is ensured that only log events older than 15 months are deleted (**FAU_STG.2**). The size of the audit trail can be configured by the Gateway Administrator using IF_GW_WAN (cf. section 7.5). Thereby the Gateway Administrator shall ensure that a sufficient amount of storage space is available to log the events within the system log for at least 15 months. In addition the TSF will ensure that there is enough storage space for a precalculated amount of events. This calculation is based on an assumption of expected events per day and a storage time of 15 months. No one is able to delete data from the system log directly. Only the authorized Gateway Administrator is able to configure the audit trail size to a smaller amount than required to store the current audit trail. The TOE ensures that only log events older than 15 months are deleted. (**FAU_STG.2**).
The **Consumer Log** informs authorized consumers about all information flows to the WAN, available Processing Profiles and billing relevant and other Meter Data. Therefore the TOE tracks all events as listed

in Table 15 (**FAU_GEN.1.1/CON**). Only authorized consumers via IF_GW_CON have the possibility to read all information from the consumer log that are related to them (**FAU_SAR.1/CON**). They have to be authenticated via username and password or via certificates (**FIA_UAU.2**). Especially the Gateway Administrator is not allowed to read the consumer log (**FDP_ACF.1.4**).
If the consumer audit trail is full, the TOE deletes a defined number of the oldest events. Whenever the TOE deletes old log events, it creates a log entry that the audit trail was cleaned up within the consumer and the system log (**FAU_STG.4/CON**). Further the Gateway Administrator, who is able to configure the size of the consumer log (cf. section 7.5), will be informed. The Gateway Administrator must ensure that a sufficient amount of storage space is available to store events within the consumer log for at least 15 months (**FAU_STG.2**). In addition the TSF will ensure that there is enough storage space for a precalculated amount of events. This calculation is based on an assumption of expected events per day and a storage time of 15 months.
Please note that nobody is able to modify the events that are recorded within the consumer log and no one is able to delete data from the consumer log directly. Only the authorized Gateway Administrator is able to configure the audit trail size to a smaller amount than required to store the current audit trail. The TOE ensures that only log events older than 15 months are deleted. (**FAU_STG.2**).
Within the **Calibration Log** only calibration relevant information as listed in Table 16 is stored (**FAU_GEN.1/CAL**).
Only the authorized Gateway Administrator via IF_GW_WAN is able to read this log file, but the TSF allow no deletions or modifications of the stored audit events (**FAU_SAR.1/CAL, FAU_STG.2**). In case that the Calibration Log is full, the TOE stops the metering operation, creates a log entry within the system log and informs the Gateway Administrator (**FAU_STG.4/CAL**). The TSF will ensure that there is enough storage space for a precalculated amount of events. This calculation is based on an assumption of expected events per day and a storage time of at least 16 years.
Within all logs, each log entry contains the information as listed in Table 14 (**FAU_GEN.1.2/SYS, FAU_GEN.1.2/CON, FAU_GEN.1.2/CAL, FAU_GEN.2**).

7.2 SF.CR: Cryptography

All connections between the TOE and external entities in WAN, HAN or LMN shall be cryptographically protected. Hence the TOE only allows TLS 1.2 protected connections according to [RFC 5246] between the TOE and entities in the WAN or HAN (**FTP_ITC.1/WAN, FTP_ITC.1/USR**). Therefore in accordance to [TR 03116-3], chapter 4.2, the TOE implements the following cipher suites (**FCS_COP.1/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, and
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384.

No other cipher suites are supported by the TOE. The corresponding key is generated using the services of the security module. The TOE itself only implements a pseudorandom function (PRF) in accordance to [RFC 5289] to generate the key from the master secret (**FCS_CKM.1/TLS**). The key size and the hash algorithm used by the PRF depend on the chosen cipher suite. As elliptical curves the TOE supports none other than the following:

- secp256r1 (prime256v1, NIST P-256) in accordance to [SECG-SEC2]
- secp384r1 (ansip384r1, NIST P-384) in accordance to [SECG-SEC2]

- brainpoolP256r1 in accordance to [RFC 5639]
- brainpoolP384r1 in accordance to [RFC 5639]
- brainpoolP512r1 in accordance to [RFC 5639]

In case that a bidirectional communication is supported by a Meter in LMN the TOE shall use the TLS protocol as described above to protect the communication between the TOE and the Meter (**FTP_ITC.1/MTR**). The usage of the TLS protocol implicitly enforces the authenticity, integrity and confidentiality of the Meter Data (**FDP_IFF.1.5/MTR**). If only a unidirectional communication to the Meter is possible, the TOE is not able to establish a TLS channel. Thus the TOE supports the following symmetric cryptographic algorithms (**FCS_COP.1/MTR**):

- id-aes128-cbc
- AES-CMAC with 128 bit key

This method enforces that the TOE and the corresponding Meter have a common symmetric 128 bit key. Since each data exchange between the Meter and the Gateway must be encrypted and MAC-protected, the TOE derives the keys k_{Enc} for encryption and k_{MAC} for MAC-Protection before any use of a new data set. Therefore the TOE supports the key generation algorithm AES-CMAC for 128bit keys in accordance to [TR 03116-3] and [RFC 4493] (**FCS_CKM.1/MTR**).
Please note that a symmetric cryptographic communication protection between Meters and TOE will only be established, if a wireless connection between the Meter and the TOE is in place or in the initial pairing of a wired Meter. However, a logically separated communication channel between the TOE and the Meter is provided regardless of whether TLS 1.2 or the symmetric cryptographic algorithm is used (**FTP_ITC.1/MTR**).
Since Meter Data intended for authorized External Entities sometimes is transferred from the Gateway via the Gateway Administrator, the content data is always encrypted for the corresponding external entity, MAC-protected and signed. For the encryption and MAC-protection of the Meter Data the TOE implements the following symmetric cryptographic algorithms (**FCS_COP.1/CMS**):

- id-aes128-GCM in accordance to [RFC 5084]
- id-aes192-GCM in accordance to [RFC 5084]
- id-aes256-GCM in accordance to [RFC 5084]
- id-aes-CBC-CMAC-128 in accordance to [TR 03109-1-I]
- id-aes-CBC-CMAC-192 in accordance to [TR 03109-1-I]
- id-aes-CBC-CMAC-256 in accordance to [TR 03109-1-I]

The randomly generated and encrypted keys for the encryption and MAC protection of the transmitted Meter Data are included in the CMS Container that is sent to the authorized External Entity. Thereby the TOE performs the Key Encryption via the following encryption algorithms in accordance to [RFC 3394]:

- id-aes128-wrap,
- id-aes192-wrap,
- id-aes256-wrap.

The key needed to perform the Key Encryption using the algorithms above is derived by the TOE using the following algorithms (**FCS_CKM.1/CMS**):

- ecka-eg-X963KDF-SHA256 in accordance to [TR 03111]
- ecka-eg-X963KDF-SHA384 in accordance to [TR 03111]
- ecka-eg-X963KDF-SHA512 in accordance to [TR 03111]

The TOE permits the following options to establish a communication via a trusted channel:

- in the WAN only the TOE is allowed to initiate the communication (**FTP_ITC.1/WAN**)
- in the HAN the consumer and service technician are allowed to initiate the communication (**FTP_ITC.1/USR**)
- in the LMN only the TOE is allowed to initiate the communication in case of a bidirectional communication. In case of a unidirectional communication the meter is allowed to initiate it (**FTP_ITC.1/MTR**)

To provide the authorized EMT with the capability to verify the origin of the received Meter Data the Gateway signs the encrypted and MAC-protected Meter Data using ECDSA in accordance to [TR 03111] with one of the hash functions SHA-256, SHA-384 or SHA-512 and one of the supported elliptic curves (**FCO_NRO.2, FCS_COP.1/HASH**). Please note that the actual signature generation is performed by the Security Module.
Further the TOE encrypts its local TSF and user data while it is stored in a persistent memory using the symmetric cryptographic algorithm XTS-AES-128 according to [IEEE P1619] with two 128-bit keys, one to encrypt the sector number represented as a 64-bit integer (plain64 mode) and the other to encrypt the tweaked payload.[52] (**FCS_COP.1/MEM**). These keys are generated using the random number generation mechanism of the Security Module and are stored permanently within the Security Module. To use the key for encryption and decryption of the persistent memory, it is loaded during boot in a secure part of the processor's RAM without user interaction. It is ensured that nobody is able to read or alter the symmetric keys used for encryption (**FDP_ACF.1.4**).
All ephemeral cryptographic keys used for TLS or symmetric AES encryption are destroyed using the method "zeroization" in accordance to [FIPS 140-2]. Therefore the TOE overrides the RAM area where those keys are stored with zeros when they are no longer needed. Please note that this RAM area is the only place where ephemeral cryptographic keys are stored (**FCS_CKM.4**).

7.3 SF.UD: User Data Protection

The TOE is attached to three separated networks HAN, WAN and LMN. The interfaces to the different networks are physically separated.
This TSF controls the access of all external entities in WAN, HAN and LMN to any information that is sent to, from or via the TOE or that is stored within the TOE. Therefore the TOE enforces two Information Flow Control Policies (**FDP_IFC.2/FW, FDP_IFF.1/FW, FDP_IFC.2/MTR, FDP_IFF.1/MTR**):

- **Firewall SFP**
  Defines the rules concerning the information flow between the different networks.
- **Meter SFP**
  Defines the handling of Meter Data by the TOE.

[52] Please note, that this does not provide the same level of security as of one 256-bit key.

and an Access Control Policy **(FDP_ACC.2, FDP_ACF.1)**:

- **Gateway SFP**
  Defines the access control policy for external entities in WAN, HAN and LMN on information maintained by the TOE.

Gateway SFP

This TSF defines the access rules for external entities based on the different roles as defined in **FMT_SMR.1**.

The TOE communicates with Meters only via the interface IF_GW_MTR (**FDP_ACF.1.2**). This interface is implemented both as a wired and a wireless interface. The wireless interface is implemented as a wM-Bus interface in accordance to [DIN EN 13757-4] and the application protocol M-Bus EN 13757-3 according to [DIN EN 13757-3] is used. The wired interface is implemented as an EIA/RS-485 interface in accordance to [TIA 485]. As application protocols the TOE supports OBIS IEC 62056-6-1 in accordance to [IEC 62056-6-1], DIN EN 13757-1 in accordance to [DIN EN 13757-1] and DLMS/COSEM IEC 65056-6-2 in accordance to [IEC 62056-6-2]. The encryption of the communication via the interface IF_GW_MTR is descibed in section 7.2.

To communicate with authorized External Entities in the HAN the TOE implements three logical interfaces:

- IF_GW_CLS,
- IF_GW_CON,
- IF_GW_SRV.

User data is provided to consumers only via the interface IF_GW_CON and Service Technicians are only able to access the TOE via IF_GW_SRV (**FDP_ACF.1.2**). Thereby the service technician is not able to read, modify or delete any TSF Data except for reading the system log. To communicate with CLS devices the TOE only uses the interface IF_GW_CLS. The physical interface to HAN is an Ethernet-Interface in accordance to [IEEE 802.3] and supports IPv4 as well as IPv6. It is realized as a 40-pin plug, and there is a module available that adapts the interface to an RJ45 plug. The communication between TOE and authorized External Entities in the HAN is secured via TLS 1.2 as described in section 7.2.

The authorized Gateway Administrator is only able to communicate with the TOE via the interface IF_GW_WAN (**FDP_ACF.1.2**). The communication is performed via RESTful COSEM web services and HTTP/1.1 according to [RFC 2616], whereby the data modelling is performed via COSEM Interface-classes according to [IEC 62056-6-1] and OBIS Codes in accordance to [IEC 62056-6-2] and [DIN EN 13757-1]. The connection is secured via TLS 1.2 as described in section 7.2.

Firewall SFP

The Firewall SFP require that only the TOE may establish a connection to an external entity in the WAN (**FDP_IFF.1.2/FW**). Therefore no connection attempts from any entities in the WAN are accepted by the TOE, except of a Wake-up call performed by an authorized Gateway Administrator (**FDP_ACF.1.2**). Therefore the Gateway Administrator prepares a Wake-up packet corresponding to the structure given in [TR 03109-1], chapter 9. Subsequently the Gateway Administrator sends this UDP packet via a preconfigured channel to the Gateway. The TOE receives the Wake-up packet and performs the following steps to check whether the packet is trustworthy:

1. The TOE checks whether the Header corresponds to the character string “WU” and whether the provided version number is supported by the TOE.
   If the verification fails the received message will be dropped and ignored. No further operations will be initiated and no feedback is provided. Otherwise the following step will be performed.

2. The TOE checks whether the given Recipient ID corresponds to the ID of TOE.
   If the verification fails the received message will be dropped and ignored. No further operations will be initiated and no feedback is provided. Otherwise the following step will be performed.

3. The TOE checks whether the time stamp provided within the Wake-up packet deviates no more than 30 seconds from the internal system time of the TOE at the time of reception by the Gateway.
   If the verification fails the received message will be dropped and ignored. No further operations will be initiated and no feedback is provided. Otherwise the following step will be performed.

4. The TOE checks whether the Wake-up packet was not received by the TOE before.
   If the verification fails the received message will be dropped and ignored. No further operations will be initiated and no feedback is provided. Otherwise the following step will be performed.

5. The TOE verifies the provided signature using the services of the Security Module.
   If the signature cannot be verified the message will be dropped and ignored. Otherwise the Gateway initiates a connection to the Gateway Administrator (**FDP_ACF.1.2, FDP_IFF.1.3/FW**). Therefore the TOE establishes a TLS channel to a pre-configured end point. Regardless whether the signature could be verified or not, the sending external entity will receive no feedback.

Further the Firewall SFP enforces that an information flow between different networks and the TOE is only allowed if the rules as described in **FDP_IFF.1/FW** are fulfilled. Otherwise the connection establishment will be denied.

Meter SFP
The Meter SFP enforce that Meter Data are provided to authorized External Entities only as defined within corresponding Processing Profiles (**FDP_IFF.1.3/MTR**). It is assumed that the Processing Profiles are correct and trustworthy. Nevertheless the TOE provides a set of tests as required in [TR 03109-1], chapter 4.4, before a Processing Profile can be activated.
In addition, this TSF monitors user data stored within the TOE for integrity errors by checking the database integrity for Meter Data and the hash value for all log data. Upon the detection of a data integrity error, the TOE informs the Gateway Administrator and creates a system log entry (**FDP_SDI.2**). Further this TSF ensures that no residual information can be accessed by an attacker. All ephemeral cryptographic keys used for TLS or symmetric AES encryption are destroyed using the method “zeroization” in accordance to [FIPS 140-2]. The TOE overwrites the memory area where those keys are stored with zeros when they are no longer needed. Furthermore, the CASA makes all TSF and user data inaccessible from TSFI as soon as they are no longer needed by only using initialized memory upon allocation, and by freeing allocated memory areas directly after use (**FDP_RIP.2**).

7.4 SF.IA: Identification & Authentication

Each user who communicates with the TOE or receives data from the TOE shall be identified and authenticated before any action on behalf of that user including receiving of data sent from the Gateway (**FIA_UID.2**, **FIA_UAU.2**). Therefore the TOE maintains the following attributes for each user (**FIA_ATD.1**):

- User Identity,
- Status of Identity (Authenticated or not),
- Connecting network (WAN, HAN or LMN),
- Role membership,

Within the process of initial association or changing of these security attributes for any user, the TOE verifies that the following rules are applied:

- if the user identity is unknown, the status of identity is set to not authenticated
- the attribute role membership shall correspond to only one of the following values or the status of identity is set to not authenticated (**FMT_SMR.1**):
  - authorized Consumer,
  - authorized Gateway Administrator,
  - authorized Service Technician,
- if the status of identity is not authenticated, neither actions on behalf of the user are executed, nor User Data is sent to the user
- if the user is an authorized Gateway Administrator the security attribute connection network shall only be WAN,
- if the user is an authorized Consumer the security attribute connection network shall only be HAN,
- if the user is an authorized Service Technician the security attribute connection network shall only be HAN,

Furthermore there must not exist more than one activated Gateway Administrator (**FIA_USB.1**). Otherwise the TOE creates an error and the corresponding value must be adjusted, before the changes are applied.
According to the attribute role membership the TOE determines the authentication mechanism that shall be used. Therefore the TOE provides the following authentication mechanisms

- 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 username and password at the IF_GW_CON interface,
- TLS-authentication via HAN-certificates at the IF_GW_SRV interface,
- authentication via HAN-certificates at the IF_GW_CLS interface,
- verification via a commands' signature.

The authentication of the Gateway Administrator and all external entities at the IF_GW_WAN interface shall only be performed via certificates that belong to the Smart Metering Public Key Infrastructure according to [TR 03109-4]. In addition, the wake-up command of the Gateway Administrator shall be authenticated by verification of the commands' signature.
In case of bidirectional communication between Meter and Gateway at the IF_GW_MTR interface the authentication of the Meter shall be performed via X.509-certificates that correspond to [TR 03109-1], chapter 10.
Consumers at the IF_GW_CON interface can decide between an authentication via certificates or via username and password. In the former case the certificates shall correspond to [TR 03109-1], chapter 11. Those certificates are also used to authenticate service technicians at the IF_GW_SRV interface and CLS at the IF_GW_CLS interface (**FIA_UAU.5**).

For the authentication mechanism via username and password the Gateway Administrator can set the threshold for unsuccessful authentication attempts[53]. Thereby the threshold shall correspond to an integer between 3 and 10 unsuccessful authentication attempts. The default value is set to 5. When the defined number of unsuccessful authentication attempts is met, the TSF informs the Gateway Administrator[54], creates a consumer log entry (if the user ID is known), creates a system log entry and locks the user account for 5 minutes (**FIA_AFL.1**). After a successful authentication of the corresponding consumer the counter of unsuccessful authentication attempts for this consumer is set to zero.
If authenticated local users in the HAN are inactive for more than 10 minutes, a re-authentication according to the authentication rules described above is required. Otherwise the next communication attempt will fail. Furthermore an established TLS channel from the TOE to the WAN shall be disconnected after 48 hours after TLS channel establishment and to the LMN after 5 MB of transmitted data (**FIA_UAU.6**).

7.5 SF.SM: Security Management

The TOE offers a set of functions to manage and configure the TSF (**FMT_SMF.1**). Those security functions comprise

- Management of devices in LMN and HAN

  The TOE provides only the authorized Gateway Administrator with the capability to register the attached devices (e.g. Meters and CLS) and to assign them to corresponding consumers (**FMT_SMR.1**).

- Client management

  The TOE provides only the authorized Gateway Administrator with the capability to create, alter and delete TOE users. Further, only the authorized Gateway Administrator is able to create and delete certificates and User ID and Password for those users (**FMT_SMR.1**).

- Maintenance of Processing Profiles

  The TOE provides only the authorized Gateway Administrator with the capability to insert, alter, activate and delete Processing Profiles.

- Key- and Certificate-Management

  The TOE provides only the authorized Gateway Administrator with the capability to insert, activate, deactivate and delete certificates for Meters, CLS, authorized External Entities and the TOE itself.

- Firmware Update

  The TOE provides only the authorized Gateway Administrator with the capability to insert, verify and activate new firmware. Before an activation of the update, the TOE checks the version number of the new firmware and verifies the integrity of the firmware update. This is done by verifying the signature using the services of the Security Module. Only if the firmware version is higher than the installed firmware version and the integrity is ensured, the TOE activates the firmware update (**FMT_MOF.1**).

- Wake-up configuration

  The TOE provides only the authorized Gateway Administrator with the capability to alter the end point which is used by the TOE to establish a TLS channel in case of a successful wake-up call.

[53] See section 7.5 for more details on the management functionality of the TOE
[54] See section 7.1 for more details.

- Monitoring

  The TOE provides only the authorized Gateway Administrator and authorized Service Technicians with the capability to read the system log. Further, only the Gateway Administrator is allowed to read the Calibration Log.

- Resetting of the TOE

  The TOE only allows the authorized Gateway Administrator to perform a reset of the SMGW. A reset is defined as an authorised reboot of the SMGW.[55] Nobody is allowed to issue a factory reset or delete all data on the SMGW.

- Audit Log configuration

  The TOE provides only the authorized Gateway Administrator with the capability to configure the size of the audit trail for the system log and the consumer log. If the audit trail is full, the oldest events get overwritten.

Especially all management functions, as listed in Table 19, and the ability to query, modify and delete the security attributes for the access control policy "Gateway access SFP" and the information flow control policies "Firewall SFP" and "Meter SFP" are restricted to the authorized Gateway Administrator and are only accessible via the interface IF_GW_WAN (**FMT_MSA.1/AC**, **FMT_MSA.1/FW**, **FMT_MSA.1/MTR** and **FMT_MOF.1**). Thereby, the restricted default values for these policies cannot be specified by any user (**FMT_MSA.3/AC**, **FMT_MSA.3/FW** and **FMT_MSA.3/MTR**).

All management functions performed by the Gateway Administrator via the IF_GW_WAN interface are performed using the "MANAGEMENT" scenario with TLS 1.2 as described in [TR 03109-1], chapter 3.2.3.1. The management functionalities for the Service Technician comprise of displaying the current time and firmware version number according to Table 18. Those management functions are performed by the Service Technician via the interface IF_GW_SRV.

The only management functions that are accessible by consumers via the interface IF_GW_CON are displaying the version number of the TOE and displaying the current time (**FMT_MOF.1**).

The TOE provides reliable time stamps by synchronizing the internal system time of the TOE according to [RFC 5905] within an interval between 90 seconds and 3 hours with a reliable external time source provided by the Gateway Administrator (**FDP_IFF.1.3/MTR**). To fulfill that requirement, the TOE supports the NTP over TLS communication protocol according to [TR 03109-1] chapter 3.2.6. Before the synchronization is applied, the TOE checks whether the deviation between the system time of the TOE and the external time source or the Round Trip Time (RTT) amounts to 3% of the shortest measuring period supported by the TOE. If the deviation time or RTT is too large, the synchronization will fail. If only the RTT was too large, another synchronization attempt is made. In the case that the deviation is too large, the TOE will stop the normal operation, create a log entry within the calibration log, inform the Gateway Administrator and enter the lock-down mode (**FDP_IFF.1.3/MTR**). Please refer to section 7.7 for more details on the lock-down mode.

In addition, the TOE contains a Real Time Clock (RTC) that shall be adjusted using the internal system time of the TOE immediately after successful synchronization with the reliable time source. The RTC is used to set the internal system time of the TOE after a power cut (**FPT_STM.1**).

7.6 SF.PR: Privacy

This TSF assures the privacy of the consumer by ensuring that authorized External Entities can only obtain data that is absolutely relevant for billing processes and the secure operation of the grid (**FPR_PSE.1.1**).

[55] Please note, that a reboot due to a temporary power loss is not an authorised reboot and as such not considered a reset.

If the identity of the consumer shall be concealed, the TOE pseudonymizes the Meter ID and ensures that no relation between the processed Meter Data and the identity of the consumer is possible. For that reason, each Processing Profile, that determines which data shall be sent to which authorized External Entity, states, whether the processed Meter Data shall be pseudonymized or not and which pseudonym shall be used if needed[56] (**FPR_PSE.1.2**). Those Processing Profiles are provided to the Gateway by the Gateway Administrator using the Management functionality of the TOE[57]. Each time when a Processing Profile is updated or a new one is added, the TOE checks whether it contains a pseudonym. If so, the TOE validates, that the pseudonym is consistent to the following alias metric (**FPR_PSE.1.3**):

- the pseudonym must not contain the Meter identity,
- the pseudonym must not contain the gateway identity,
- the pseudonym must not contain the Consumer identity,

If this validation fails, the TOE informs the Gateway Administrator and does not activate this Processing Profile.
If Meter Data shall be provided pseudonymized to an authorized EMT, the TOE removes the unique Meter ID and replaces the ID by the pseudonym given within the Processing Profile. Subsequently, the data is encrypted and signed for the authorized EMT as described within the Processing Profile[58]. Afterwards, the encrypted and signed data is transmitted to the Gateway Administrator as described within the Processing Profile. The Gateway Administrator shall verify the signature, remove the signature and send the encrypted data to the authorized EMT. Since the signature of the Gateway is removed, the authorized EMT has no possibility to relate the received meter data to any consumer (**FPR_PSE.1.1**).
Further, the TOE provides the possibility to conceal the frequency of Meter Data sent to authorized External Entities to ensure that no information of consumer behavior can be obtained by the analysis of the load or size of Meter Data or the frequency (including the absence) of sending it (**FPR_CON.1.1**). The TOE connects to the authorized EMT as defined within the Processing Profile in an interval configurable by the Gateway Administrator between one minute and one year (**FPR_CON.1.2**).

7.7 SF.SP: Self-protection

The TOE provides a set of self-protection mechanisms that, in particular, comprises the self test of the TOE, detection of replay attacks and the failure with preservation of a secure state.
Within the self test functionality, the TOE implements different tests, such as the verification of HAN/WAN separation, which are used to define the system's health status (**FPT_TST.1**, **FPT_SDI.2**). Those tests can be grouped in three categories:

- periodically running tests
- tests running inside the modules
- detection of possible tampering events based on log entries

The periodically running tests are also used to verify the system during the boot process. Those test are performed in the background every 24 hours per default. Furthermore the self test can be triggered by an authenticated user (consumer, service technician, gateway administrator) to check the integrity of the TSF and the TSF data. Each TOE software module implements a module-specific self test function which

[56] According to **A.ProcessProfile**, it is assumed that the Processing Profiles are trustworthy and correct.
[57] See section 7.5 for more details on the Management functionality of the TOE.
[58] See section 7.2 for more details on the encryption algorithm and process.

is invoked by the periodically running general tests. To detect tampering events, the TOE analyzes the system log for an unusual amount of error messages and other anomalies.

In addition, the TOE provides a set of mechanisms against replay attacks. Therefore, the TOE ensures that only TLS-protected connections are possible between the TOE and devices located in the WAN, HAN or LMN (except for Meters where only a unidirectional communication is possible, cf. section 7.2). TLS[59] protects the TOE from replay attacks. To detect replay attacks of unidirectional communication in the LMN, the TOE checks whether the transmission counter of the received data is greater than the previous one. In case of Wake-up calls, the TOE verifies that the attached time stamp is not older than 30 seconds and that this Wake-up packet was not received before. Otherwise, the packet will be dropped and ignored (**FPT_RPL.1**).

To preserve a secure state even in case of a failure or attack, this TSF provides a lock-down mode of the TOE, which is used to prevent an attacker from gaining information about the device configuration and the device itself (**FPT_FLS.1**). In this lock-down mode, the system shuts down all functions including the metering operation but except those needed to contact the Gateway Administrator and display a warning to the consumer. The only way to return to the normal operation mode is a reset initiated by the Gateway Administrator.

The TOE enters the lock-down mode, if one of the following events occur:

- an integrity error within the TSF data occurred during a periodically running test (**FPT_TST.1**)
- an integrity error within the user data occurred during a periodically running test (**FPT_SDI.2**))
- the deviation between the internal system time and the reliable time source exceeds 3% of the shortest measuring period supported by the TOE
- the calibration log has reached its limit
- other critical errors occurred

A list of all critical error codes and all possible integrity errors can be found in [AGD Gateway Administrator und Servicetechniker, chapter 11.6].

The Gateway has affixed a seal in a way, that it is not possible to open the casing of the Gateway without visible tampering of the seal. The ventilation louvers are placed in a way that it is not possible to attach to the Debug and JTAG interfaces of the TOE without opening the casing. Those are mounted on the concealed side of circuit board (**FPT_PHP.1**). Furthermore, the Debug and JTAG interface are disabled after production of the Gateway.

7.8 Rationale on TOE Specifications

	SF.AU	SF.CR	SF.UD	SF.IA	SF.SM	SF.PR	SF.SP
FAU_ARP.1/SYS	X						
FAU_GEN.1/SYS	X						
FAU_SAA.1/SYS	X						
FAU_SAR.1/SYS	X						

[59] For more information on the TLS-protocol refer to section 7.2.

	SF.AU	SF.CR	SF.UD	SF.IA	SF.SM	SF.PR	SF.SP
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					
FDP_ACC.2			X				
FDP_ACF.1	X	X	X				
FDP_IFC.2/FW			X				
FDP_IFF.1/FW			X				
FDP_IFC.2/MTR			X				
FDP_IFF.1/MTR		X	X		X		
FDP_RIP.2			X				
FDP_SDI.2			X				X
FIA_ATD.1				X			
FIA_AFL.1				X			

	SF.AU	SF.CR	SF.UD	SF.IA	SF.SM	SF.PR	SF.SP
FIA_UAU.2	X			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		
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		
FPT_TST.1							X
FPT_PHP.1							X
FTP_ITC.1/WAN		X					
FTP_ITC.1/MTR		X					
FTP_ITC.1/USR		X					

Table 24: Fulfilment of Security Requirements

8. Appendix

8.1 Mapping from English to German terms

English term	German term
billing-relevant	abrechnungsrelevant
CLS, Controllable Local System	dezentral steuerbare Verbraucher- oder Erzeugersysteme
Consumer	Anschlussnutzer Letztverbraucher (im verbrauchenden Sinne) u.U. auch Einspeiser
Consumption Data	Verbrauchsdaten
Gateway	Kommunikationseinheit
Grid	Netz (für Strom/Gas/Wasser)
Grid Status Data	Zustandsdaten des Versorgungsnetzes
LAN, Local Area Network	Lokales Netz (für Kommunikation)
LMN, Local Metrological Network	Lokales Messeinrichtungsnetz
Meter	Messeinrichtung (Teil eines Messsystems)
Meter Profile	Zählerprofil
Processing Profiles	Konfigurationsprofile
Security Module	Sicherheitsmodul (z.B. eine Smart Card)
Service Provider	Diensteanbieter
Smart Meter Smart Metering System[60]	Intelligente, in ein Kommunikationsnetz eingebundene, elektronische Messeinrichtung (Messsytem)
TOE	EVG (Evaluierungsgegenstand)
WAN, Wide Area Network	Weitverkehrsnetz (für Kommunikation)

[60] Please note that the terms “Smart Meter” and “Smart Metering System” are used synonymously within this document

8.2 Glossary

Term	Description
8p8c	8 position 8 contact connector
AES	Advanced Encryption Standard
Authenticity	property that an entity is what it claims to be (according to [SD6])
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 [SD6])
Consumer	End user of electricity, gas, water or heat. (according to [CEN]), See chapter 3.1
CPU	Central Processing Unit
DLMS	Device Language Message Specification (originally Distribution Line Message Specification)
EAL	Evaluation Assurance Level
EMT	Externer Marktteilnehmer, authorized External Entity in the WAN which receives Meter Data from the TOE
external entity	See chapter 3.1
FAKRA D	50 ohm radio frequency interface (RFI) for road vehicles (50 Ohm RFI) acc. DIN 72594-1 and USCAR-18 ("FAachKReis Automobil")
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
GPRS	General Packet Radio Service
GSM	Global System for Mobile
HDLC	High-Level Data Link Control
Home Area Network (HAN)	In-house LAN which interconnects domestic equipment and can be used for energy management purposes. (according to [CEN])
HTTP	HyperText Transfer Protocol

Term	Description
HTTPS	HyperText Transfer Protocol Secure
Integrity	property that sensitive data has not been modified or deleted in an unauthorised and undetected manner (according to [SD6])
LAN	Local Area Network
LED	Light-emitting diode
Local attacker	See chapter 3.4
MAC	Message Authentication Code
MB	Mega Byte
M-Bus	Meter-Bus
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 analyzing large quantities of Meter Data. ([CEN])
Meter Profile	A Meter Profile contains the configuration for the Gateway which is necessary to communicate with a Meter and retrieve Meter data (cf. [TR 03109-1, ch. 4.4.2])
NTP	Network Time Protocol
OMS	Open Metering System
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.

Term	Description
pseudorandom function (PRF)	Function to generate the key for TLS from the master key
RAM	Random Access Memory
REST	Representational State Transfer
RFI	radio frequency interface
RS-485	Standard defining the electrical characteristics of drivers and receivers for use in balanced digital multipoint systems, also known as EIA-485.
RTC	Real Time Clock
Service Technician	See chapter 3.1
SFP	Security Functional Policy
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SML	Smart Message Language
Tariff	Price structure (normally comprising a set of one or more rates of charge) applied to the consumption or production of a product or service provided to a consumer. (according to [CEN])
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security protocol according to RFC5246
TOE	Target of Evaluation – set of software, firmware and/or hardware possibly accompanied by guidance
TSF	TOE security functionality
UART	Universal Asynchronous Receiver Transmitter
WAN attacker	See chapter 3.4
wM-Bus	wireless M-Bus

Bibliography

[TR 03109-1] Version 1.0. BSI, 18.03.2013 (cit. on pp. 10, 11, 15, 16, 33, 36, 40, 67, 73, 80, 105, 109–111, 113, 120).

[AGD Gateway Administrator und Servicetechniker] *CASA 1.0(CASA-AGD), Installations- und Konfigurationshandbuch für Service-Techniker Gateway-Administrator*. Version 1.18. EMH metering GmbH & Co. KG, Mar. 2020 (cit. on p. 115).

[TR 03109] *BSI TR-03109*. Version 1.0.1. BSI, 11.11.2015 (cit. on pp. 1, 2).

[TR 03109-1-I] *BSI TR-03109-1 Anlage I: CMS Datenformat für die Inhaltsdatenverschlüsselung und -signatur*. Version 1.0. BSI, 18.03.2013 (cit. on pp. 24, 70, 107).

[TR 03109-1-VI] *BSI TR-03109-1 Anlage VI: Betriebsprozesse*. Version 1.0. BSI, 18.03.2013 (cit. on p. 27).

[TR 03109-3] *BSI TR-03109-3: Kryptographische Vorgaben für die Infrastruktur von intelligenten Messsystemen*. Version 1.1. BSI, 17.04.2014 (cit. on pp. 15, 24, 32, 42, 71).

[TR 03109-4] *BSI TR-03109-4: Smart Metering PKI - Public Key Infrastruktur für Smart Meter Gateways*. Version 1.2. BSI, 9.12.2016 (cit. on p. 111).

[TR 03111] *BSI TR-03111: Elliptic Curve Cryptography (ECC)*. Version 2.10. BSI, 1.06.2018 (cit. on pp. 68, 69, 108).

[TR 03116-3] *BSI TR-03116-3: Kryptographische Vorgaben für Projekte der Bundesregierung. Teil 3: Intelligente Messsysteme*. BSI, 4.04.2016 (cit. on pp. 106, 107).

[CC] *Common Criteria for Information Technology Security Evaluation –*
- *Part 1: Introduction and general model, dated April 2017, version 3.1, Revision 5*
- *Part 2: Security functional requirements, dated April 2017, version 3.1, Revision 5*
- *Part 3: Security assurance requirements, dated April 2017, version 3.1, Revision 5*

. (Cit. on pp. 6, 28, 50, 78).

[SMGW-PP] *Common Criteria Protection Profile for a Gateway for Smart Metering Systems (BSI-CC-PP-0073)*. Version 1.3. BSI, 31.03.2014 (cit. on pp. 1–3, 7, 9, 17, 18, 28).

[DIN EN 13757-1] *DIN EN 13757-1: Kommunikationssysteme für Zähler, Teil 1: Datenaustausch*. DIN, 2014 (cit. on p. 109).

[DIN EN 13757-3] *DIN EN 13757-3: Kommunikationssysteme für Zähler und deren Fernablesung, Teil 3: Spezielle Anwendungsschicht*. Norm. DIN, Aug. 2013 (cit. on p. 109).

[DIN EN 13757-4] *DIN EN 13757-4: Kommunikationssysteme für Zähler und deren Fernablesung, Teil 4: Zählerauslesung über Funk (Fernablesung von Zählern im SRD-Band)*. Norm. DIN, Nov. 2013 (cit. on p. 109).

[TIA 485] *Electrical Characteristics of Generators and Receivers for Use in Balanced Multipoint Systems*. Revision A. TIA, 1998, reaffirmed 2003 and 2012 (cit. on p. 109).

[TR 03109-1 Errata TAF9/10] *Errata für die BSI TR-03109-1 v1.0.1 - TAF 9 und TAF 10*. Version 1.0. BSI, 12.12.2019 (cit. on p. 67).

[IEC 62056-6-1] *IEC 62056-6-1: Datenkommunikation der elektrischen Energiemessung - DLMS/COSEM - Teil 6-1: COSEM Object Identification System (OBIS)*. IEC, June 2017 (cit. on p. 109).

[IEC 62056-6-2] *IEC 62056-6-2: Datenkommunikation der elektrischen Energiemessung - DLMS/COSEM - Teil 6-2: COSEM Interface-Klassen*. IEC, June 2017 (cit. on p. 109).

[IEEE 802.3] *IEEE 802.3 Ethernet Working Group - IEEE Standard for Ethernet*. IEEE, 2012 (cit. on p. 109).

[IEEE P1619] *IEEE P1619™/D16 Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices*. IEEE, May 2007 (cit. on pp. 72, 108).

[RFC 2616] *IETF RFC 2616, R. Fielding et al.: Hypertext Transfer Protocol - HTTP/1.1*. IETF, 1999 (cit. on p. 109).

[RFC 3394] *IETF RFC 3394, J. Schaad, R. Housley: Advanced Encryption Standard (AES) Key Wrap Algorithm*. IETF, 2002 (cit. on pp. 69, 107).

[RFC 3565] *IETF RFC 3565, J. Schaad: Use of the Advanced Encryption Standard (AES) Ecryption Algorithm in Cryptographic Message Syntax (CMS)*. IETF, 2003 (cit. on p. 70).

[RFC 4493] *IETF RFC 4493, J. H. Song, J. Lee, T. Iwata: The AES-CMAC Algorithm*. IETF, 2006 (cit. on pp. 70–72, 107).

[RFC 5084] *IETF RFC 5084, R. Housley: Using AES-CCM amd AES-GCM Authenticated Encryption in the Cryptographic Message Syntax (CMS)*. IETF, 2007 (cit. on pp. 70, 107).

[RFC 5246] *IETF RFC 5246, T. Dierks, E. Rescorla: The Transport Layer Security (TLS) Protocol Version 1.2*. IETF, 2008 (cit. on pp. 68, 106).

[RFC 5289] *IETF RFC 5289, E. Rescorla: TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)*. IETF, 2008 (cit. on pp. 68, 69, 106).

[RFC 5639] *IETF RFC 5639, M. Lochter, J. Merkle: Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation*. IETF, 2010 (cit. on pp. 68, 69, 107).

[RFC 5905] *IETF RFC 5905, D. Mills, et al.: Network Time Protocol Version 4: Protocol and Algorithms Specification*. IETF, 2010 (cit. on pp. 77, 113).

[SD6] *ISO/IEC JTC 1/SC 27 N7446, Standing Document 6 (SD6): Glossary of IT Security Terminology*. ISO/IEC, Apr. 2009. URL: http://www.jtc1sc27.din.de/sce/sd6 (cit. on pp. 119, 120).

[FNN Log] *Lastenheft Logmeldungen zur Einbindung von SMGw-G1-Geräten*. Version 1.00. VDE (FNN), 14. Juni 2016 (cit. on pp. 55, 60).

[RFC 2104] *Network Working Group RFC 2104, H. Krawczyk et al.: HMAC: Keyed-Hashing for Message Authentication*. Network Working Group, Feb. 1997 (cit. on pp. 68, 69).

[FIPS 140-2] *NIST FIPS PUB 140-2: Security Requirements for Cryptographic Modules, Part 2*. NIST, 2001 (cit. on pp. 72, 108, 110).

[FIPS 180-4] *NIST FIPS PUB 180-4: Secure Hash Standard (SHS)*. NIST, 2015 (cit. on pp. 68, 69, 72).

[FIPS 197] *NIST FIPS PUB 197: Announcing the ADVANCED ENCRYPTION STANDARD (AES)*. NIST, 2001 (cit. on pp. 69–72).

[NIST SP800-38A] *NIST SP800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques*. NIST, 2001 (cit. on pp. 69–71).

[NIST SP800-38B] *NIST SP800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*. NIST, 2005 (cit. on pp. 70, 71).

[NIST SP800-38D] *NIST SP800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC*. NIST, 2007 (cit. on pp. 69, 70).

[SM-PP] *Protection Profile for the Security Module of a Smart Meter Gateway (BSI-CC-PP-0077-V2)*. Version 1.03. BSI, 11.12.2014 (cit. on pp. 3, 6, 8, 9, 23, 28, 35, 41).

[PTB A50.7] *PTB A50.7: Physikalisch-Technische Bundesanstalt: Anforderungen an elektronische und softwaregesteuerte Messgeräte und Zusatzeinrichtungen für Elektrizität, Gas, Wasser und Wärme*. PTB, 2002 (cit. on p. 8).

[PTB A50.8] *PTB A50.8: Physikalisch-Technische Bundesanstalt: Smart Meter Gateway*. PTB, 2014 (cit. on pp. 1, 2, 64, 65).

[CEN] *SMART METERS CO-ORDINATION GROUP (SM-CG) Item 5. M/441*
first phase deliverable – Communication – Annex: Glossary. SMCG/Sec0022/DC, 2011 (cit. on pp. 4–6, 119–121).

[SECG-SEC2] *Standards For Efficient Cryptography 2 (SEC2): Recommended Elliptic Curve Domain Parameters*. Version 2.0. Standards for Efficient Cryptography Group (SECG), 27.01.2010 (cit. on pp. 68, 69, 106).